NIPES

Journal of Science and Technology Research

Journal homepage: www.nipesjournals.org.ng

Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech)

[1]Malasowe, Bridget Ogheneovo, [2]Aghware, Fidelis Obukohwo, [3]Okpor, Margaret Dumebi, [4]Edim, Edim Bassey, [5]Rita Erhovwo Ako, [6]Arnold Adimabua Ojugo

[1,2]Department of Computer Science, Faculty of Computing, University of Delta, Agbor, Delta State, Nigeria
[3]Department of Cyber Security, Faculty of Computing, Delta State University of Science and Technology, Ozoro. Nigeria
[4]Department of Computer Science, Faculty of Physical Science, University of Calabar, Calabar, Nigeria
[5,6]Department of Computer Science, College of Science, Federal University of Petroleum Resources Effurun, (FUPRE), Delta State, Nigeria
Email : [1]bridget.malasowe@unidel.edu.ng, [2] fidelis.aghware@unidel.edu.ng, [3]okpormd@dsust.edu.ng, [4]edime@unical.edu.ng, [5]ako.rita@fupre.edu.ng [6]ojugo.arnold@fupre.edu.ng

Article Info

Keywords: *cybersecurity, educational technology, strategies, best practices, risk*

Received 4 March 2024
Revised 17 May 2024
Accepted 22 May 2024
Available online 30 June 2024

https://doi.org/10.5281/zenodo.12617068

Abstract

In order to effectively manage the risk and hazards associated with the online environment, there is a growing demand for cyber security awareness due to the rising use of the Internet and the concerning rise in cyberattacks. The types of cybersecurity risks, best practices and current approaches for controlling cybersecurity threats in educational technology settings are examined in this paper and, we also examined effective cybersecurity case studies. The results show that a variety of cybersecurity threats are faced by educational institutions. These threats include phishing, ransomware attacks, insider threats, malware, social engineering, Distributed Denial of Service (DDoS), vulnerabilities, credential theft, IoT , man-in-the-middle, third-party vendor risks among others. Institutions must implement proactive, effective cybersecurity strategies in order to reduce these risks. These strategies include risk assessments, the creation of strong cybersecurity governance frameworks, multi-factor authentication (MFA), frequent software updates and patch management, robust access controls, data encryption, frequent backups, incident response plans, network segmentation, monitoring, and logging, cyber insurance, and the deployment of access controls and encryption mechanisms. The integration of several cybersecurity strategies, including as vulnerability management, incident response planning, security awareness training, and continuing training programs, is highlighted in the successful case studies. Educational institutions may secure sensitive data, defend against cyberattacks, and guarantee the public's access to secure, continuous education by putting comprehensive cybersecurity strategies and best practices into place. The outcomes of this investigation offer significant perspectives and suggestions for academic establishments and interested parties about the handling of cybersecurity hazards in EdTech settings.

1. Introduction

The way students learn and interact in educational contexts has changed dramatically in recent years because to the increased adoption of educational technology, or EdTech [1]. The term "edtech"

refers to a wide range of digital tools, platforms, and applications that improve the way educational content is delivered, encourage communication, and offer individualized learning opportunities. While EdTech has many advantages, such easier access to educational materials and higher levels of participation, it also brings with it new difficulties, especially when it comes to cybersecurity threats. In order to enhance teaching and learning activities, educational institutions of all stripes—from basic schools to universities are depending more and more on digital platforms and online services. These developments in technology have opened up new avenues for learning outside of the traditional classroom, including asynchronous and distant learning. The availability, confidentiality, and integrity of sensitive data may be jeopardized, and educational institutions are now more vulnerable to a broad range of cybersecurity risks as a result of this digital revolution. Protecting sensitive data, including student records, financial information, and research data, is essential in educational environments. Because educational institutions manage and preserve a substantial amount of sensitive and personal data, they are attractive targets for cybercriminals. A breach in cybersecurity can have major consequences, including financial losses, reputational damage, and legal duties. Cyber incidents can also create a great deal of disturbance to the educational process, affecting not only students but also teachers and administrative staff.

Institutions need to implement comprehensive strategies and best practices to manage cybersecurity threats in educational technology environments [2]. Data security is becoming a skill and is of utmost importance, network managers now need to be ready to employ a variety of drastic actions to safeguard data and the network system [3][4]. These strategies must to be in line with accepted cybersecurity frameworks and standards while addressing the particular difficulties and demands of the educational sector. Educational institutions can secure sensitive data, defend against cyberattacks, and guarantee the continuation of instructional services by putting strong cybersecurity measures in place. The first step of the research is to examine how educational technology is developing and the cybersecurity threats that come with it. It explores the several kinds of dangers that educational institutions have to deal with, such as ransomware attacks, phishing scams, insider threats, and data breaches. The study will draw attention to the possible repercussions of these cyber incidents and how they affect the learning process.

Additionally, the study looks at the essential elements of a thorough cybersecurity plan for academic institutions. It discusses the significance of risk assessment and management, emphasizing the necessity of approaching cybersecurity pro-actively and preventively. The research will examine the importance of putting in place a strong cybersecurity governance framework as well as the duties and obligations of different stakeholders, including administrators, IT personnel, and educators. The study also highlights the significance of staff awareness and training initiatives as a critical component of cybersecurity readiness. It looks at how faculty and students can safeguard confidential data, encourage responsible online conduct, and spot and report possible security issues. The study also addresses the function of recovery planning and incident response in lessening the effects of cybersecurity incidents. In order to enhance future cybersecurity procedures, it will examine how crucial it is to create and test incident response plans, set communication protocols, and carry out post-event analysis. The educational sector has benefited greatly from the quick development of educational technology. But it has also made educational institutions more vulnerable to cybersecurity threats, which call for careful and proactive management. The goal of this research is to offer tactics and best practices that educational institutions can use to safeguard confidential data, lessen cyberattacks, and guarantee the uninterrupted and secure provision of educational services. Educational institutions may establish a safer digital environment for administrators, professors, and students by putting these guidelines into practice.

1.1 A Cyberattack's Anatomy

We must break down a cyberattack into its component parts in order to comprehend its complexities. A typical cyberattack can be divided into a few essential stages that shed light on the strategies used

by the malicious actor and how their attack unfolds [5]. Figure 3 illustrates how the attack begins with target identification, data collection, the actual cyberattack, and the subsequent investigation.

a) Identifying: The bad actor gathers information about the target in the first step. This recon mission may involve mapping out the network architecture, investigating possible points of entry, and locating weaknesses in the target's systems. To identify these vulnerabilities, attackers frequently use social engineering, publicly accessible data, and scanning technologies.
b) The use of weapons: Malicious software, such as viruses or malware, must be created or obtained during this phase in order to exploit the vulnerabilities that have been found. Creating a potent weapon that can be utilized to interfere with the target's systems is the goal.
c) Transport: At this point, the weaponized payload is delivered by the attacker across the target's network or devices. Different delivery methods are used, such as via malicious links and email attachments, as well as taking use of software flaws. The aim is to gain entry into the target's network and establish a presence there.
d) Misuse of power: In this phase, the attacker takes advantage of weaknesses to obtain unapproved entry. This could entail exploiting unpatched systems, weak passwords, or software flaws. After gaining access, the attacker aims to increase privileges and move stealthily through the network.
e) Setup: The attacker installs more malware or tools after acquiring access in order to stay persistent within the compromised system. This guarantees ongoing authority and the capacity to carry out additional tasks, such obtaining confidential information or initiating new assaults.
f) Control and direction: The attacker can take control of the compromised systems remotely by setting up a command and control infrastructure. In order to execute orders, exfiltrate data, and maintain control, a communication channel must be established between the attacker's infrastructure and the penetrated network during this phase.
g) Objective-driven actions: Once control has been gained, the attacker can focus on achieving their main goals. Depending on why the attacker is doing it, this could involve data theft, service interruptions, or other nefarious acts.

The purpose of this study is to investigate the methods and approaches that work best for controlling cybersecurity threats in learning technology environments. This study intends to offer insights and recommendations to educational institutions and stakeholders involved in the implementation and administration of EdTech solutions by reviewing recent literature, case studies, and expert comments.

2.0 Literature Review

The use of educational technology (EdTech) in educational environments has witnessed significant growth in recent years. Cyber security involves taking proactive measures to protect data from external and internal threats and to protect networking. In order to facilitate the implementation of alternate delivery methods, such as asynchronous learning, in the Nigerian educational system, [49] developed a virtual learning framework. As a result, professionals are primarily concerned with protecting computers, networks, servers, and intranets. [35] clarified that data accessibility is facilitated by cyber security, which verifies the legitimacy of individuals. Understanding the many forms of cyber security is now essential to improving data protection. Examining the state of research on cybersecurity risk management in educational technology environments is the goal of this assessment of the literature, with an emphasis on tactics and best practices used by educational establishments. A variety of academic papers, reports, and case studies are also included in the

review to offer insights into the difficulties faced by educational institutions and the practical steps that may be taken to reduce cybersecurity threats.

2.1 Threats from Cybersecurity and the Changing Environment of Educational Technology

Access to educational resources has been improved and learning opportunities have increased with the inclusion of EdTech into educational environments. Nevertheless, cybersecurity threats have also been brought about by this digital revolution. The expanding significance of cybersecurity in educational technology environments is emphasized [6], who also stress the necessity to address the particular issues that educational institutions confront in securing sensitive data. Cybersecurity risks that affect educational institutions are diverse and include ransomware attacks, phishing scams, insider threats, and data breaches. [7] stress how important it is to comprehend these dangers and the possible outcomes. They contend that detecting vulnerabilities and putting in place suitable security measures depend heavily on a proactive approach to risk assessment and management. In order to mitigate cybersecurity concerns, educational institutions need to implement all-encompassing measures. [8] emphasize the significance of instituting a cybersecurity governance framework that delineates the duties and responsibilities of all parties engaged in the execution and administration of education technology solutions. They stress that in order to guarantee a comprehensive strategy to cybersecurity, administrators, IT personnel, and educators must work together.

Figure 1. The anatomy of a cyber-attack [9][10][11]

2.2 Methods and best practice for managing cybersecurity issues in educational sector.

The way educational institutions provide learning experiences has been completely transformed by educational technology. However, there are serious cybersecurity dangers associated with the use of technology in education. The following are best practices in managing cybersecurity issues in EdTech environment by different scholars:

- Security Awareness Campaigns: Keep users informed about cybersecurity best practices [3].
- Training Programs: Regular training sessions enhance cybersecurity awareness [4].
- Continuous Monitoring: Ensures real-time detection of suspicious activities [8].
- Environmental Controls: Protect physical infrastructure from environmental damage [10].
- Automated Patch Deployment: Ensures timely application of updates [11].
- Anomaly Detection: Identifies unusual behavior indicating potential threats [15].
- Application Testing: Identifies vulnerabilities before deployment [16].
- Patch Management: Efficient patch management prevents exploitation of known vulnerabilities.

- **Data Encryption**: Encryption safeguards sensitive data during transmission and storage. Encryption at rest, encryption in transit, and end-to-end encryption are important techniques. Encryption in Transit: Utilizing TLS/SSL protocols ensures data security during transmission [19]
- Surveillance Systems: Monitor and deter unauthorized activities [21].
- Access Controls: Prevent unauthorized physical access to sensitive areas [26]
- Third-Party Audits: Provides an objective security assessment from external experts [27].
- Secure Development Practices: Adopting secure coding and conducting code reviews prevent security flaws [31].
- Phishing Simulations: Educate users on recognizing phishing attacks [40].
- Encryption at Rest: Encrypting stored data with robust algorithms like AES-256 protects against unauthorized access [41].
- Centralized Logging: Collects and analyzes logs from various sources for threat detection [42].
- **Access Control and Identity Management**: Effective access control and identity management are fundamental to securing EdTech environments. Role-Based Access Control (RBAC) restricts access based on user roles, thereby minimizing unnecessary access [24]. Single Sign-On (SSO) simplifies user authentication processes and reduces password fatigue [44] It is essential to use methods like Single Sign-On (SSO), Role-Based Access Control (RBAC), and Multi-Factor Authentication (MFA). Multi-Factor Authentication (MFA) enhances security by requiring multiple forms of verification [46].
- Regular Updates: Keeping software up-to-date is crucial for security [48].
- Incident Response Plan: Outlines procedures for responding to security incidents [52].
- Backup Testing: Ensures that data can be restored when needed [53].
- Firewalls: Monitor and control network traffic based on security rules [59].
- Compliance: Adherence to regulations like FERPA, GDPR, and ISO/IEC 27001 ensures legal compliance [56].
- Intrusion Detection and Prevention Systems (IDPS): Detect and prevent malicious activities [57].
- End-to-End Encryption: Ensures data remains encrypted throughout its lifecycle [62]
- Post-Incident Analysis: Identifies root causes and prevents future incidents [62].
- Patch Management Policy: Establishes guidelines for managing updates and patches [63].
- Web Application Firewalls (WAFs): Protect web applications from common attacks [64]
- Security Policies: Comprehensive policies ensure consistent cybersecurity practices [64]
- Risk Management: Regular risk assessments guide security efforts [65].
- Automated Vulnerability Scanning: Continuously monitors systems for new vulnerabilities [66]
- Virtual Private Networks (VPNs): Secure remote access to educational networks [66].
- Incident Response Team: Ensures quick and effective handling of incidents [67][70].
- Network Security: Protecting the network infrastructure is vital for maintaining a secure EdTech environment.
- User Education and Awareness Educating users about cybersecurity is critical for reducing human error-related risks.
- Incident Response and Management: To lessen the effects of security breaches, a clearly defined incident response plan is necessary.
- Data Backup and Recovery: Consistent data backups and comprehensive recovery strategies guarantee data availability and integrity. Frequent Backups: Schedule backups to guard against data loss. [68].
- Disaster Recovery Plan: Facilitates swift restoration of operations post-incident [69].

- Application Security: Secure application development practices prevent vulnerabilities in educational software.
- Monitoring and Recording: To identify and address security concerns, ongoing monitoring and recording are crucial.
- Regular Security Audits and Vulnerability Assessments are essential for identifying and mitigating security risks. Penetration Testing: Identifies and addresses vulnerabilities through simulated attacks [71].
- Policy and Governance: Strong policy and governance frameworks are crucial for maintaining security standards.
- Physical Security: Physical security measures protect the infrastructure supporting EdTech environments.

To improve cybersecurity readiness, educational institutions must also fund staff training and awareness initiatives. According to [32], faculty members and students are essential in safeguarding private data and encouraging responsible online conduct. They stress the necessity of continual training programs to inform users about possible online dangers and offer advice on how to keep secure online spaces. Protecting educational technology settings requires the implementation of robust security mechanisms. Institutions should emphasis the importance of secure network topologies, encryption techniques, and access controls during the implantation of IT in the institution. To stop fraudsters from taking advantage of vulnerabilities, they advise routinely upgrading software and patching them. The significance of utilizing cloud-based security solutions to improve data protection is also emphasized by the researchers. Educational institutions must have clear incident response and recovery procedures in place in case of a cybersecurity incident. According to [36][43], minimizing the effects of a cyber event requires a prompt and well-coordinated reaction. In order to enhance future cybersecurity procedures, they stress the necessity of routinely testing incident response strategies, efficient communication methods, and post-event analysis. Numerous academic establishments have effectively employed cybersecurity tactics to safeguard their technological surroundings. The University of California, Davis, for instance, created an information security program that combined incident response, vulnerability management, and security awareness training [56]. A proactive cybersecurity framework was established at the University of Texas at Austin, with an emphasis on risk assessment, incident response, and continuous training programs [1]. These case studies offer insightful analysis and useful suggestions for other educational establishments. [44] presented a visual model of methods to elucidate relevant techniques (Figure 2). The review of the literature identifies the various cybersecurity dangers that the education sector faces and emphasizes the growing significance of risk management for cybersecurity in educational technology systems. Numerous cybersecurity issues that affect educational institutions might have serious repercussions if they are not promptly and appropriately addressed using the appropriate strategy. Educational institutions can strengthen their cybersecurity posture and safeguard sensitive data by putting comprehensive strategies and best practices into place, such as creating a cybersecurity governance structure, holding frequent security training and awareness programs, Multi-Factor Authentication (MFA), Regular Software Updates and Patch Management, Robust Access Controls, Data Encryption, Regular Backups, Incident Response Plan, Network Segmentation, Monitoring and Logging, Third-Party Risk Management, Mobile Device Management (MDM), and Cyber Insurance. The review's case studies show how these actions are both achievable and efficient.

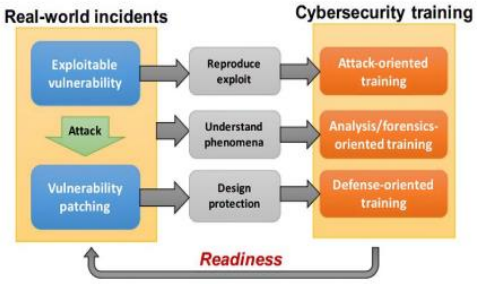

Figure 2: Paradigm of strategies [45]

3. 0 Methodology

This study employed a systematic review methodology to look at the approaches and best practices for managing cybersecurity threats in educational technology environments. A thorough and meticulous analysis of the body of available literature was made possible using the systematic review methodology. The stages involved in carrying out the systematic review are described in the sections that follow.

3.1 Research Design

Establishing the study's goals and research questions was part of the research design. "What are the strategies and best practices for managing cybersecurity risks in educational technology environments?" was the main study topic. Investigating the components of effective cybersecurity strategies, examining successful case studies of cybersecurity implementation in educational technology environments both inside and outside of Nigeria, and identifying the types of cybersecurity threats that educational institutions face were some of the objectives.

3.2 Literature search from academic databases

A methodical search approach was created to guarantee an exhaustive and complete review. A combination of keywords and controlled vocabulary terms were used to search several electronic databases, including academic databases (Table 1). Variants of "cybersecurity", ”cybersecurity strategies”, ”cybersecurity current trends”, "educational technology", "risk management", "best practices" and similar terms were among the search terms used in the database search.

Table 1: Academic data base

S/NO	Name Of Database	Discipline(s)	Description
1	Internet Archive Scholar	Multidisciplinary	Focuses on full-text journal and conference proceedings searches in open access
2	CORE	Multidisciplinary	An all-inclusive full text aggregator for open access publications for journals and repositories (institutional, subject, preprints, etc.). over 20 million active users each month.
3	CiteSeerX	Multidisciplinary	Swap out ChemXSeer and CiteSeer. mostly mathematics, statistics, and computer science.
4	Paperity	Multidisciplinary	Over 17,000 open access journals from various academic areas are aggregated in full text format.
5	ResearchGate	Multidisciplinary	Researcher and scientist social networking site on a business basis. More than 19 million users have enrolled and are sharing

			datasets, publications, and other research products.
6	HAL	Multidisciplinary	A French researcher's open-access database. divided into a domain portal and an institution.
7	ERIC: Educational Resource Information Center+A19	Education	Resources and literature in education going back to 1966
8	Synthical	Multidisciplinary	Preprints mostly in the fields of biology, chemistry, statistics, and computer science.
9	Zendy	Multidisciplinary	Emphasis is on academic content, such as books, book chapters, conference proceedings, full-text papers, and indexed journals from open access sources. There are 38 languages available for the content, which covers a range of topics and specialties.
10	Aminer	Computer Science	An online tool for indexing and searching social networks within academia
11	BASE: Bielefield Academic Search Engine	Multidisciplinary	260 million documents' worth of metadata from over 8,000 content providers
13	CNKI	Multidisciplinary	A Chinese bibliographic database
15	Crossret+A21	Multidisciplinary	An official International DOI Foundation Digital Object Identifier (DOI) Registration Agency. Information on grants, preprints, articles, datasets, and journals from 17,633 members (publishers, journals, etc.)
17	Dimensions	Multidisciplinary	Preprints, conference proceedings, books and book chapters, publications, and patents as well as clinical trials and policy documents are all connected to one another. based on CrossRef. includes Altmetric attention scores and citation-based metrics.
18	Directory of Open Access Journals (DOAJ)	Multidisciplinary	18,652 open access journals article
19	DBLP	Multidisciplinary	An extensive collection of papers from prestigious computer science publications and conferences
20	Google Scholar	Multidisciplinary	The largest academic search engine and database (estimated at around 390 million records, unofficially)
21	J-Gate+A	Multidisciplinary	An electronic gateway to the world's electronic journal literature, J-Gate offers articles from 58,000 publications.
22	The Lens	Multidisciplinary	serves the public interest by providing global patent and academic information to support science- and technology-enabled problem solutions.
23	MyScienceWork	Multidisciplinary	Over 90 million scientific publications and 12 million patents are included in the database.
25	OAIster+A34	Multidisciplinary	Over 1,500 organizations have submitted cover records.
26	OpenAIRE Graph	Multidisciplinary	Scientific Understanding A key component supporting the European Open Science Cloud is a graph that aggregates, duplicates, and enriches the metadata of publications, research data, software, and other products.

			It also includes relationships to donors and awards.
27	OpenAlex	Multidisciplinary	Every academic output's index and metadata
29	ScienceOpen	Multidisciplinary	Humanities, social sciences, and physical and natural sciences. includes PubMed, SciiELO, and arXiv. integrated with Altmetrict UIDs from ORCID. papers from more than 25,000 publications.
30	Scopus	Multidisciplinary	Data from more than 5,000 foreign publishers and more than 20,500 titles
31	Web of Science	Multidisciplinary	Includes the Zoological Record, Biological Abstracts, Science Citation Index, and Social Science Citation Index.
33	Academic Search	Multidisciplinary	Multiple editions: Premier, Elite, Complete, and Alumni Edition
34	African Journals OnLine (AJOL)	Multidisciplinary	academic publications released in Africa
36	Cabells	Multidisciplinary	database for searching, evaluating, and comparing journals. Journal listings contain information on metrics, submission guidelines, and publication data.
37	Current Conttents	Multidisciplinary	a section of the scientific web. comprised of seven discipline-specific subgroup.
38	DSI: Stutttgart_Database_of_Scientific _lllustrators	Multidisciplinary	Bio bibliographic information with 20 search fields on illustrators of scientific works published between approximately 1450 and 1950
40	Information Bridge: Department of Energy Scientific and Technical Information	Multidisciplinary	offers more than 266,000 full-text papers and bibliographic citations of Department of Energy (DOE) research report literature for free to the general public. The majority of the documentation dates from 1991 onward.
41	Indian Citation Index	Multidisciplinary	Cover articles from more than a thousand Indian scientific, technical, medical, and social science journals
42	IARP	Multidisciplinary	Open-access information management system for the natural and social & behavioral sciences that includes funding, publications, and conferences
44	JournalSeek	Multidisciplinary	lists the content from over 39,000 journals, including the ISSN, subject area, description, goals, scope, journal abbreviation, and homepage URL.
45	Jurn	Multidisciplinary	Appropriately index and provide open access to publications in the fields of business, economics, ecology, science, biology, and the humanities
46	Mendeley	Multidisciplinary	Research document database sourced from the public. The researchers uploaded more than 100 million documents and added data from repositories (including PubMed and arXiv).
47	ORCID	Multidisciplinary	an impartial, public registry for identifying contributors to research and scholarly publications. List: peer review, works, grants, education,

			biography, and employment. more than 9.3 million profiles.
48	Publons	Multidisciplinary	Academics can use this service to keep track of their editorial contributions to academic journals and peer reviews. Combining Researcher-ID with
49	Science.gov	Multidisciplinary	An entry point to government science data and research findings culled from more than 2,200 webpages, 60 databases, and 200 million pages.
50	Science Citation Index	Multidisciplinary	A portion of Science Wednesday. more than 24,000 journals in 254 different academic areas.
51	Scientific Information Database (SID)	Engineering & Technology, Medical Science, Basic Science, Human Science	An Iranian academic journal index providing full text or metadata access
52	SCInddeks – Serbian Citation Index	Multidisciplinary	An electronic publishing platform, an Open Access full-text journal repository, a national citation index, and a bibliographic database. more than 230 journals' articles
53	SNAC (Social Network and Archival Contexts)	Multidisciplinary	Archival materials directory arranged by subject entity
55	Ulrich's Periodicals Directory	Multidisciplinary	offers serials for publications
56	WorldCat	Multidisciplinary	unified catalog of catalogs from participating libraries
57	WorldWideScience	Multidisciplinary	a combined catalog listing 17,900 libraries' holdings across 123 nations
58	Association for Computing Machinery Digital Library	Computer Science, Engineering	Compilation of all ACM publications, including books, technical magazines, newsletters, conferences, proceedings, and journals
59	IEEE Xplore	Computer Science, Engineering, Electronics	Over 5 million records.
60	IngentaConnect	Multidisciplinary	Includes content from 13,000 journals.
61	JSTOR:Journal Storage	Multidisciplinary	Books, journal articles, and original materials in 75 fields (1870-present)
62	OpenEdition.org	Humanities, social science	provides four global publishing and information platforms for the social sciences and humanities (10,661 books, 549 journals, 3793 blogs, and 45,591 events).
63	SciELO	Multidisciplinary	A concept and database for cooperative electronic publication in underdeveloped nations, mostly in Africa and South America. Over 1700 journals are indexed
64	SpringerLink	Multidisciplinary	Books, periodicals, protocols, reference materials, journals, and proceedings

3.3 Review Selection

Inclusion and exclusion criteria were utilized to select relevant studies for the systematic review. The inclusion criteria encompassed peer-reviewed journal publications, conference papers, reports, and case studies that were released between the years 2001 and 2023.. Research on cybersecurity

risk management in educational technology environments was necessary, as was the provision of best practices and methods.

3.4 Data cleaning and Extraction

There are two stages to the screening process: full-text screening comes after title and abstract screening. Two independent reviewers assessed the titles and abstracts of the chosen studies based on the inclusion and exclusion criteria. All disputes were resolved by discussion and consensus. The remaining studies were put through full-text screening to see if they could be included in the review. To extract the relevant data from the selected research, a standardized form was employed. The information that was obtained contained bibliographic data, study techniques, significant conclusions, and recommendations about cybersecurity strategies and best practices in educational technology settings. Two reviewers carried out the data extraction procedure separately.

3.5 Data Analysis

A thematic approach was employed for the analysis of the data gathered from the chosen research. It was determined which major themes and supporting themes there were for cybersecurity tactics and best practices. As part of the analysis, the gathered data was categorized into meaningful groups, and the connections between various themes were examined. The results of the chosen studies were combined to determine recurring themes, new directions in cyberattack research, and effective mitigation strategies.

4.0 Presentation of Results

In this section, the findings from the systematic review of types of cyberattacks and best practices for managing cybersecurity risks in educational technology environments are presented. The findings are arranged according to three main themes: categories of cybersecurity threats, components of effective cybersecurity strategies, and instances of effective cybersecurity integration in educational technology environment. The research questions and objectives were addressed in an organized manner by the systematic review's findings. The findings were arranged thematically, emphasis on the different kinds of cybersecurity risks that are prevalent in educational institutions that they must deal with, the elements of successful cybersecurity plans, and the successful case studies that have been found in the literature. Summaries from the chosen studies were used as evidence to support the review finding the sources.

4.1 Types of Cybersecurity Threats in Educational Technology Environment (ETE)

In the context of educational technology environments (ETE), the systematic research revealed a variety of cybersecurity concerns that educational institutions must contend with. The main conclusions for each kind of threat are outlined in the subsections that follow. Due to the large volume of sensitive data educational institutions handle, these ranges from financials, student's academic data, and research data to the personal information of students and staff, educational institutions are becoming more and more vulnerable to cyberattacks and proactive step must be taken to curb the ever increasing cyberattacks to institutional databases. Some frequent forms of cybersecurity threats that educational institutions encounter are as follows:

1. **Malware:** Software intended to harm or interfere with systems. This include malware that can penetrate institutional networks, such as worms, trojans, and viruses. [5].
2. **Unpatched Software Vulnerabilities:** Taking advantage of security holes in out-of-date software that hasn't been patched or updated. Attackers frequently use this as a point of entry. [13]

3. **Man-in-the-Middle (MitM) Attacks:** Without the parties' knowledge, listening in on and maybe changing their conversations, which could jeopardize critical information [14].
4. **Cyber Espionage:** Targeted assaults intended to steal sensitive data, research findings, and intellectual property from universities conducting cutting-edge research [17].
5. **Mobile Device Threats:** Potential hazards to staff and students' mobile devices include viruses, phishing apps, and unsecured Wi-Fi networks. [23].
6. **Social Engineering:** Strategies employed to coerce someone from disclosing private information. Pretexting, baiting, and other dishonest tactics fall under this category. [33].
7. **Credential Theft:** Theft of usernames and passwords to obtain unauthorized access to institutional systems, frequently via keylogging or phishing [34].
8. **IoT Attacks:** Taking advantage of holes in Internet of Things (IoT) devices—such as thermostats, smart cameras, and other linked devices—that are connected to the institution's network. [38]
9. **Ransomware:** Malicious malware that encrypts data belonging to institutions and requests a ransom to unlock. This has the potential to seriously impair educational processes [39].
10. **Distributed Denial of Service (DDoS) Attacks:** Overloading University servers with so much traffic that it interferes with online services like email, webpages, and learning management systems. [45]
11. **Insider Threats:** Malevolent acts by personnel or students who abuse their access to systems and data within the organization.
12. **Data Breaches:**Unauthorized access to private information, including financial records, personal details, and student records. Weak security procedures or insider threats may be at blame for these breaches [53]
13. **Advanced Persistent Threats (APTs):** Prolonged and focused cyberattacks, in which hackers hide inside a network for a lengthy time with the intention of stealing information or spying on activities [54].
14. **Phishing Attacks: Phishing emails**- Phishing emails are fraudulent emails that aim to fool recipients into opening malicious attachments or disclosing private information. Also, **spear Phishing**-Targeted phishing assaults directed towards certain people, frequently administrators or high-ranking officials. [54].
15. **Third-Party Vendor Risks:** Dangers associated with outside vendors and services having access to networks and institutional data. Security lapses may have an effect on the organization. [57].

4.2. Effective Cybersecurity Strategies to mitigate threat

Several essential elements of successful cybersecurity tactics in learning technology environments were found in the review. The results pertaining to each component are described in the subsections that follow.

a) **Regular Backups:** Institutions should create routine data backups and ensure that backups are kept in a safe location. This can help with data recovery in the event of a ransomware attack or other situation involving data loss[6].
b) **Monitoring and Logging:** Ascertain continuous network operations tracking and recording to detect and handle any anomalous activity as soon as possible [9].
c) **Network Segmentation:** To prevent malware from spreading and unauthorized users from accessing the network, divide the institutional network into sections [18].
d) **Data Encryption:** Encrypt sensitive data both in transit and at rest to prevent unauthorized access**.** [27].
e) **Regular Software Updates and Patch Management:** To guard against known vulnerabilities, ensure that all systems and software are routinely patched and updated [30].

f) **Incident Response Plan:** Establish and maintain a thorough incident response plan to quickly address and mitigate cybersecurity risks [39].
g) **Regular Security Training and Awareness Programs:** Provide staff and students with regular training sessions to teach them how to recognize and handle cybersecurity threats including phishing and social engineering assaults [55].
h) Multi-Factor Authentication (MFA): To access institutional systems and improve security beyond the use of passwords alone, employ multi-factor authentication (MFA).
i) Sturdy Access Controls: Strict access control protocols must to be implemented to ensure that only authorized users can access sensitive data and systems.
j) **Third-Party Risk Management:** o Evaluate and control the risks related to third party vendors and service providers having access to systems and data within the institution. [57].
k) **Mobile Device Management (MDM):** Implement mobile device management (MDM) tools to control and safeguard staff and student mobile devices and ensure they follow security guidelines.
l) **Cyber Insurance:** To reduce monetary damages brought on by cybersecurity disasters, cyber insurance should be a vital option to purchase [62].

In the educational sector, combining technical solutions for the aforementioned security risks with policy implementations and ongoing education and awareness campaigns is the most efficient and significant cybersecurity approach. These are best practices in today ever developing world in terms of technology. When these best practices are used, they form a strong cybersecurity framework that can successfully defend educational institutions against a variety of cyber threats.
The study underscores the necessity for educational establishments to rapidly implement integrated technical measures in a timely manner. By addressing existing vulnerabilities and guarding against new ones, this will lower the likelihood that cyberattacks will be successful.

4.3. Effective Case Studies on Cybersecurity Implementation in Global Education Systems.

Due to the paucity of published literature on the topic, it can be difficult to locate successful case studies that are especially focused on cybersecurity implementation in educational institutions in Nigeria and globally. It is possible to highlight some generic case studies and cybersecurity initiatives that have been successful in Nigeria and other nations. They are as follows:

a) **Lagos State University (LASU) Cybersecurity Program:** Lagos State University has started programs to raise staff and student knowledge of cybersecurity, including regular security workshops and the addition of cybersecurity sections to their IT curriculum. [2]
b) **University of Delta, Agbor (UNIDEL): The** State University has taken proactive steps to train staffs and students on cybersecurity. A thorough cybersecurity plan has also been put in place to secure the University portal management system.
c) **Case Study: Covenant University Cybersecurity Initiatives:** Covenant University has put in place a thorough cybersecurity plan that makes use of intrusion detection systems, firewalls, and frequent cybersecurity audits. The university places a strong emphasis on cybersecurity instruction and research. [7].
d) **Case Study: Australian Universities Cybersecurity Network**: In order to improve their cybersecurity posture, Australian universities have established a cooperative network that includes pooled resources, coordinated attack response, and cooperative training initiatives [12].
e) **Case Study: University of Nigeria's Cybersecurity Measures:** The University of Nigeria has adopted cutting-edge security technologies, collaborated with international cybersecurity organizations, and regularly trained staff and students as part of its proactive cybersecurity efforts. [20].

f) **National Efforts and Policies:** Nigeria's National Information Technology Development Agency (NITDA) has been creating national policies and frameworks to improve cybersecurity across several industries, including education. National Information Technology Development Agency [48]
g) **Case Study: Cybersecurity in UK Higher Education Institutions**: Comprehensive cybersecurity policies have been established by UK higher education institutions, which include the creation of cybersecurity centers, partnerships with business, and curricular integration for cybersecurity education [48].
h) **Case Study: Cybersecurity Framework in Singapore's Education Sector:** Strict security guidelines, frequent audits, and cybersecurity awareness training for employees and students are all part of the national cybersecurity framework that Singapore's Ministry of Education has put in place [57].
i) **Case Study: Cybersecurity Measures in the United States K-12 Schools:** Strong cybersecurity precautions have been put in place by a number of K–12 schools in the US, including the usage of firewalls, network monitoring, and student cybersecurity education initiatives.
j) **Case Study: Cybersecurity Strategy in Canadian Universities:** In order to safeguard its IT infrastructure, Canadian colleges have implemented a thorough cybersecurity policy that includes incident response planning, ongoing security training, and cutting-edge technology solutions [58].
k) **Case Study: South African Universities' Cybersecurity Readiness**: Universities in South Africa have put cybersecurity readiness programs into place, emphasizing risk management, policy creation, and frequent training for end users and IT personnel [61].

The above case studies offer insightful information about how educational institutions in Nigeria and other nations are tackling cybersecurity issues by combining cooperative initiatives, policies, and instructional initiatives. In order to improve cybersecurity in educational institutions, the case studies also emphasize the significance of all-encompassing cybersecurity plans, ongoing education and awareness campaigns, and national policy support.

5.0 Findings

The results of the systematic review demonstrated the wide variety of cybersecurity risks that educational institutions must contend with while using educational technology. Comprehensive cybersecurity policies are necessary, given the various dangers that have been uncovered, including ransomware attacks, phishing scams, insider threats, and data breaches. For educational institutions to effectively counter these dangers, they must take a proactive and preventive stance immediately as the approach of the cyberattacks is changing by the day. The results of the systematic research show how critical it is that educational institutions prioritize cybersecurity and put comprehensive plans and best practices into place. By being aware of the various cybersecurity threats they face and having appropriate countermeasures in place, educational institutions may secure sensitive data, lower risks, and ensure the safe and continuing provision of educational services. The review's conclusions provide incisive analysis and practical recommendations for educational institutions and those interested in tackling cybersecurity concerns in educational technology environments.
.

6.0 Discussions

The review identification of the elements of successful cybersecurity strategies offers educational institutions a road map for improving their cybersecurity posture. The focus on risk management and assessment draws attention to how crucial it is to comprehend the unique risks and vulnerabilities that each organization faces. Educational institutions can efficiently allocate resources and prioritize efforts to mitigate identified hazards by performing regular assessments.

The implementation of a cybersecurity governance framework guarantees a synchronized and uniform strategy towards cybersecurity. Preventive measures and prompt responses to security crises are made possible by good communication channels, clear roles and duties, and collaboration amongst many stakeholders. This cooperative strategy cultivates a cybersecurity culture in educational establishments. Programs for employee awareness and training have become essential parts of cybersecurity tactics. Learning about cybersecurity threats and best practices can help educational institutions build a human firewall that protects against cyberattacks. Frequent training programs and role-playing games raise awareness, encourage appropriate online conduct, and provide people the tools they need to recognize and report security incidents.

Encryption, frequent software updates, and strict access controls are necessary to safeguard educational technology environments. These steps address known vulnerabilities, restrict illegal access, and lessen the effect of future data breaches. Updating software and systems allows educational institutions to effectively defend against new threats. The review's case studies offer real-world instances of effective cybersecurity deployment in learning contexts. Some educational institutions across the world have shown the benefits of comprehensive programs that include a variety of cybersecurity measures, such as security awareness training, vulnerability management, incident response planning, and ongoing training initiatives. These case studies demonstrate how important leadership participation, teamwork, and ongoing development in preserving a robust cybersecurity posture. It's crucial to recognize the systematic review's limitations, though. The review was restricted to studies and publications that published between 2004 and 2023. The review also depended on the quality and accessibility of the included papers, as well as their possible publication.

6.1 The consequences of cyber security risks encountered in the education sector

The repercussions of cybersecurity risks in the educational industry are far-reaching. These are the following: Identity theft and financial loss can result from data breaches and privacy concerns; Significant privacy violations may arise from unauthorized access to personal information and private communications; Distributed Denial of Service (DDoS) attacks have the potential to interfere with online learning, tests, and resource access; Operational Impact assaults have the potential to interfere with administrative processes, impacting salaries and admissions alike; Ransomware attacks are becoming more common in schools, where the attackers lock down computers and demand money to unlock them; Institutions must incur substantial costs in order to strengthen their cybersecurity defenses and recover from assaults; The trust that employees, parents, and students have in an institution can be eroded by data breaches and cyber disasters. Unfavorable press coverage can damage the school's reputation and have an impact on students; Cyberattacks may result in intellectual property and academic records being accessed and altered without authorization, which could compromise the institution's integrity; Cybersecurity risks have far-reaching effects on the educational industry, including data protection, financial stability, operational continuity, reputation, and legal compliance. Comprehensive cybersecurity policies must be implemented by educational institutions in order to reduce these threats and safeguard their communities.

7.0 Conclusion

It is imperative for the education sector to put comprehensive cybersecurity policies into place in order to safeguard confidential data, uphold confidence, and guarantee the provision of educational services. Technical fixes, policy initiatives, and ongoing training and awareness campaigns can all be combined to help educational institutions strengthen their cybersecurity posture and better fend off changing cyberattacks.

The best strategies and tactics for controlling cybersecurity threats in technologically-enhanced learning environments were examined in this study. The research determined the types of cybersecurity threats that educational institutions face globally, looked at the elements of successful cybersecurity strategies, and provided case studies of successful cybersecurity implementation through a methodical analysis of the body of existing literature. The study's findings highlight the diverse range of cybersecurity dangers that educational institutions have to contend with, including insider threats, phishing scams, ransomware attacks, and data breaches. The consequences of these attacks are severe and multifaceted, affecting financial stability, operational efficiency, data privacy, reputation, legal compliance, and the psychological well-being of individuals that are connected to the educational sector. To reduce these risks, educational institutions must create thorough incident response plans, put strong cybersecurity measures in place, and encourage a culture of cybersecurity awareness. To reduce these dangers and safeguard sensitive data, educational institutions must take preventative action. Integration of multiple essential elements is necessary for effective cybersecurity tactics in educational technology environments. Prioritizing risk mitigation initiatives, assessing the impact of threats, and detecting vulnerabilities all depend heavily on risk assessment and management. The implementation of a strong cybersecurity governance framework guarantees cooperation among many stakeholders, delineates roles and duties, and expedites the prompt handling and resolution of security issues. The implementation of a strong cybersecurity governance framework guarantees cooperation among many stakeholders, delineates roles and duties, and expedites the prompt handling and resolution of security issues. Successful case studies demonstrating the successful application of cybersecurity in educational technology environments were also identified by the systematic review. These case studies demonstrated the importance of comprehensive programs that included a variety of cybersecurity measures, including security awareness training, vulnerability management, incident response planning, and ongoing training initiatives. The success of these implementations was predominantly ascribed to collaboration, active involvement of the leadership, and continuous enhancement of cybersecurity best practices within the educational domain.

References

[1] Ashley, C., & Preiksaitis, M. (2022). Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises. *Business Management Research and Applications: A Cross-Disciplinary Journal*, *1*(2), 109-157.

[2] Akinyemi, O. T., & Akinyemi, O. O. (2020). Enhancing cybersecurity education in Nigerian universities: A case study of Lagos State University. *Nigerian Journal of Technology, 39*(1), 90-98. https://doi.org/10.4314/njt.v39i1.10

[3] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787

[4] Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312. https://doi.org/10.1016/j.chb.2014.05.046

[5] Aycock, J. (2006). Computer viruses and malware. Springer. https://doi.org/10.1007/978-0-387-30236-2

[6] Ahmed, M., & Ullah, S. (2017). Effective data backup using data deduplication techniques. 2017 International Conference on Communication, Computing and Digital Systems (C-CODE), 204-208. https://doi.org/10.1109/C-CODE.2017.7918960

[7] Adebayo, F. O., & Tiamiyu, A. O. (2019). Cybersecurity management in tertiary institutions in Nigeria: A case study of Covenant University, Ota. International Journal of Computer Applications, 178(15), 29-34. https://doi.org/10.5120/ijca2019918755

[8] Barrett, M. (2005). Security Operations Center: Building, Operating, and Maintaining Your SOC. Cisco Press.

[9] Bejtlich, R. (2013). *The practice of network security monitoring: Understanding incident detection and response*. No Starch Press.

[10] Blyth, A., & Kovacich, G. L. (2001). Information assurance: Security in the information environment. Springer.

[11] Brumfield, M., & Dunne, E. (2014). Patch management: Keeping your network secure. Network Security, 2014(2), 11-13. https://doi.org/10.1016/S1353-4858(14)70015-4

[12] Cornish, L. (2018). Collaborative cybersecurity initiatives among Australian universities. *Australian Journal of Information Systems, 22*(1), 1-15. https://doi.org/10.3127/ajis.v22i0.1721
[13] Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2008). Security patch management: Share the burden or share the damage? Management Science, 54(4), 657-670. https://doi.org/10.1287/mnsc.1070.0768
[14] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051. https://doi.org/10.1109/COMST.2016.2548426
[15] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1-58. https://doi.org/10.1145/1541880.1541882
[16] Chess, B., & McGraw, G. (2004). Static analysis for security. IEEE Security & Privacy, 2(6), 76-79. https://doi.org/10.1109/MSP.2004.97
[17] Carr, J. (2011). Inside cyber warfare: Mapping the cyber underworld. O'Reilly Media.
[18] Cisco Systems. (2016). Network segmentation design guide. Cisco Systems. https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html
[19] Dierks, T., & Rescorla, E. (2008). The Transport Layer Security (TLS) protocol version 1.2. RFC 5246. https://doi.org/10.17487/RFC5246
[20] Emenike, S. O., Olatunji, O. M., & Emudainohwo, O. B. (2018). Cybersecurity awareness and knowledge in tertiary institutions in Nigeria: Case study of the University of Nigeria, Nsukka. *Journal of Educational and Social Research, 8*(1), 91-100. https://doi.org/10.2478/jesr-2018-0009
[21] Fennelly, L. J. (2012). Effective physical security. Elsevier.
[22] Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability engineering & system safety, 121, 90-103.
[23] Felt, A. P., Egelman, S., Finifter, M., Akhawe, D., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In Proceedings of the eighth symposium on usable privacy and security (p. 3). https://doi.org/10.1145/2335356.2335360
[24] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC), 4(3), 224-274. https://doi.org/10.1145/501978.501980
[25] Fuchs, E. P., Aldawood, A., & Skinner, B. (2021). *Managing Cybersecurity Risks in Educational Technology Environments*. Routledge.
[26] Garfinkel, S., & Spafford, G. (2002). Web security, privacy & commerce. O'Reilly Media, Inc.
[27] Hayes, B. (2016). Third-Party Audits: Internal Auditors Assess Value. Internal Auditor, 73(6), 55-61.
[28] Glipa, C. G., Ignacio, R. A., Alvez, G. U., Guilot, R. T., & Sasan, J. M. (2023). Implication of Individual Plan for Professional Development (IPPD) on Teachers' Professional Development and Career Advancement. *Web of Semantic: Universal Journal on Innovative Education*, *2*(6), 43-54.
[29] Ghosh, S., & Turrini, E. (2010). *Cryptography and network security*. Springer. https://doi.org/10.1007/978-0-387-87816-4
[30] Hsu, C. H., & Wang, S. L. (2015). An empirical study on improving software security patch management. *Information and Software Technology, 57*, 77-88. https://doi.org/10.1016/j.infsof.2014.07.007
[31] Howard, M., & Lipner, S. (2006). The security development lifecycle. Microsoft Press.
[32] Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.
[33] Hadnagy, C. (2010). Social engineering: The art of human hacking. Wiley.
[34] Herley, C., & Florêncio, D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. Economics of Information Security and Privacy, 33, 33-53. https://doi.org/10.1007/978-1-4419-6967-5_3
[35] Jamal, A., Abdullah, A. J., Ibrahim, I. M., & Akin, E. (2021). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *10*(12), 1456. https://doi.org/10.3390/electronics10121456
[36] Kilag, O. K. T., Angtud, R. M. A., Uy, F. T., Alvez, G. G. T., Zamora, M. B., Canoy, C. B., & Sasan, J. M. (2023). Exploring the Relationships among Work Motivation, Job Satisfaction, Administrative Support, and Performance of Teachers: A Comprehensive Study. *International Journal of Scientific Multidisciplinary Research*, *1*(3), 239-248.Kilag, O. K. T., Bariquit, I. A.,
[37] Killcrece, G., Kossakowski, K. P., Ruefle, R., & Zajicek, M. (2003). *Incident management: Establishing an incident response capability*. Carnegie Mellon University, Software Engineering Institute. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305
[38] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84. https://doi.org/10.1109/MC.2017.201
[39] Kharraz, A., Robertson, W. K., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. Detection of Intrusions and Malware, and Vulnerability Assessment, 9148, 3-24. https://doi.org/10.1007/978-3-319-20550-2_1

[40] Jansson, K., & Von Solms, R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584-593. https://doi.org/10.1080/0144929X.2011.632650
[41] Katz, J., & Lindell, Y. (2020). Introduction to modern cryptography. CRC Press.
[42] Kent, K., & Souppaya, M. (2006). Guide to Computer Security Log Mangement. National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
[43] Kilag, O. K. T., Evangelista, T. P., Sasan, J. M., Librea, A. M., Zamora, R. M. C., Ymas, S. B., & Alestre, N. A. P. (2023). Promising Practices for a Better Tomorrow: A Qualitative Study of Successful Practices in Senior High School Education. *Journal of Elementary and Secondary School*, *1*(1).
[44] Khan, B., & Al-Yasiri, A. (2016). *Identifying requirements for a cloud-based single sign-on solution*. Journal of Cloud Computing, 5(1), 1-13.
[45] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emergingtrends and recent developments. *Energy Reports*, *7*, 8176-8186.
[46] McGettrick, A. (2013). Toward effective cybersecurity education. Security and Privacy Magazine, 11(6), 66-68. https://doi.org/10.1109/msp.2013.155
[47] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53. https://doi.org/10.1145/997150.997156
[48] Microsoft Microsoft Entra multifactor authentication overview - Microsoft Entra ID | Microsoft Learn. Visited June 2024
[49] Malasowe, B. O., Akazue, M. I., Okpako, E. A., Aghware, F. O., Ojie, D. V., & Ojugo, A. A. (2023). Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities. International Journal of Advanced Computer Science and Applications, 14(8), 135–142. https://doi.org/10.14569/IJACSA.2023.0140816
[50] Ojugo, A. A., & Yoro, R. E. (2021b). Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack. International Journal of Electrical and Computer Engineering, 11(2), 1498–1509. https://doi.org/10.11591/ijece.v11i2.pp1498- 1509
[51] Ojugo, A. A., & Yoro, R. E. (2020a). Forging A Smart Dependable Data Integrity And Protection System Through Hybrid-Integration Honeypot In Web and Database Server. Technology Report of Kansai University, 62(08), 5933–5947
[52] National Information Technology Development Agency (NITDA). (2019). *National Cybersecurity Policy and Strategy*. Federal Republic of Nigeria. Retrieved from https://nitda.gov.ng/wp-content/uploads/2019/03/National-Cybersecurity-Policy-and-Strategy.pdf
[53] National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce.
[54] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, *52*, 194-206. https://doi.org/10.1016/j.cose.2015.02.008
[55] Persons, O., Butavicius, M. A., Pattinson, M., McCormac, A., & Jerram, K. (2015). *The human aspect of information security and assurance - a pilot study on phishing*. In Proceedings of the 16th European Conference on Cyber Warfare and Security (pp. 241-248). Academic Conferences Limited.
[56] Ponemon Institute. (2020). Cost of a data breach report 2020. IBM Security. https://www.ibm.com/security/data-breach
[57] Sasan, J. M., Barquin, A. M. E., Alestre, N. A., Librea, A., & Zamora, R. M. (2022). Karl Marx on technology and alienation. *Science and Education*, *3*(9), 228-233.
[58] Tuma, F. (2021). The use of educational technology for interactive teaching in lectures. *Annals of Medicine and Surgery*, *62*, 231-235.
[59] Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security*, *2011*(8), 16-19. https://doi.org/10.1016/S1353-4858(11)70086-1
[60] Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, 101666.
[61] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 Proceedings IEEE INFOCOM* (pp. 1-9).
[62] Rains, T. (2015). *Third-party vendor risk management: Reduce your risk*. Microsoft. https://info.microsoft.com/third-party-vendor-risk-management
[63] Renaud, K., & Goucher, W. (2016). Cybersecurity strategy in Canadian higher education institutions. *Canadian Journal of Higher Education*, *46*(4), 56-73. https://doi.org/10.47678/cjhe.v46i4.186604
[64] Ristenpart, T., & Yilek, S. (2018). *The value and limits of end-to-end encryption*. Communications of the ACM, 61(6), 56-63.
[65] Stallings, W. (2016). *Network security essentials: Applications and standards* (6th ed.). Pearson.
[66] Stuttard, D., & Pinto, M. (2011). *The web application hacker's handbook: Finding and exploiting security flaws* (2nd ed.). Wiley

[67] Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). *Risk management guide for information technology systems* (NIST Special Publication 800-30). National Institute of Standards and Technology.
[68] Tafa, Z., & Jashari, A. (2011). Mobile device management and security. *2011 International Conference on High Performance Computing & Simulation*, 717-721. https://doi.org/10.1109/HPCSim.2011.5999873
[69] The anatomy of cybersecurity attack: insight into modern security. https://www.acronis.com/en-us/blog/posts/anatomy-of-a-cyberattack-insights-into-modern-security-threats/#
[70] Tan, W. K., & Goh, T. T. (2019). Enhancing cybersecurity in Singapore's education sector. *Computers & Security*, *85*, 65-75. https://doi.org/10.1016/j.cose.2019.04.004
[71] Werlinger, R., Hawkey, K., Muldner, K., Jaferian, P., & Beznosov, K. (2010). *The challenges of using an intrusion detection system: Is it worth the effort?* In Proceedings of the 7th Symposium on Usable Privacy and Security (pp. 1-12).