THE JOURNAL OF ARTS, HUMANITIES AND DEVELOPMENT STUDIES RESEARCH (JAHDSR)

Volume 6, Issue No.2, pp 103-110, June, 2025
www.researchersjournal.org
E-Mail: jahadsresearch@gmail.com
info@researchersjournal.org
Received April, 2025, Accepted May, 2025, published: June, 2025

Cyber security and Online Data in Nigerian Education: Challenges/ Prospects.

[1]Ushie, C. A., [1]Ayah, G. B. & [2]Ushie, B. C.
Department of Educational Technology, University of Calabar, Nigeria
E-mail: beshelushie1117gmail.com
gracebasseyayah@gmail.com, https//orcid.org/0000-0003-0799-5314
Dept. of Environmental Education, University of Calabar, Nigeria
christieushie1@gmail.com; https://orcid.org/0000-0003--0862-2165.

Abstract

The education industry, just like any other sphere of human endeavours has been infiltrated by technology with far reaching consequences. For instance, sources of information have grown to include varied types of online or digital tools resulting in information explosion in the cyber space. These sources of information are often exposed to unwarranted exploitation by dubious members of society, hence the need for their preservation. This paper used the review design to examine what already exists and recommends that institutions of learning should among other things provide regular training programme for the staff a students to be able to handle their cyberspaces effectively. This paper therefore examined the concept of cyber security, its aspects in education, importance, consequences for its neglect and best practices that educational institutions can adopt to stay afloat in all their activities for maximum productivity in the field of education.

Key words: *Cybersecurity, online data, education, digital tools, challenges, prospects.*

Introduction

Nigeria currently runs a 9-3-4 system of education in which learners spend nine years in what is generally referred to as Basic education, three years of senior secondary and four years at the tertiary level of either college, polytechnic or university education. At these various levels, there are registered data including but not limited to personnel, facilities and equipment needed for the smooth operations of the education sub-systems. For instance, the National Bureau of Statistics (2024) stipulates that there are not less than 10.5 million children registered in primary schools

across the country. These children's data such as Date/ Place of Birth, names of parents and such other information are recorded and stored in the cloud for future reference. There are other data in the system such as intellectual property research findings, qualitative and quantitative information from teachers, administrators and other stakeholders, test scores, graduation rates ,etc that needs to be preserved for reference purposes.

Cyber security in education according to Bryan, (2024) refers to the practices, techniques and policies designed to protect: (a) educational institution's networks, systems and data from unauthorised access, use, disclosure, disruption, modification or destruction (b) sensitive information including student's records such as grades, personal details, teachers' and other staff information, research data and financial transactions. (c) Also included are online learning platforms, digital resources and educational technologies. Some of the specifics are student generated contents as assignments, projects, e-books, videos, Students Information Systems (SIS) and Learning Management systems (LMS).

Chancey , (2023) refers to cybersecurity in education to mean all the methods, measures and practices implemented to protect the availability, integrity and confidentiality of sensitive data of educational institutions. It also involves developing different security protocols and training school staff and students to mitigate cyber threats. These normally aimed at changing or damaging important information accessing and extorting money from the owners via ransom ware or interrupting normal business transactions.

Aspects of cyber security threat in education

Some key aspects of cyber security in online education data are:

1. **Data Breaches:** This refers to unauthorised access to sensitive information such as students' records, financial information or personal identification information. This exposes the legitimate owners to untold hardships as the infiltrators may use such information to extort money or expose them to public ridicule.

2. **Phishing attacks:** Uses fraudulent emails, email attachments, text messages or phone calls that trick users into revealing login details, credentials or sensitive information. It exists in the forms of Spear, Whale or Business Email Compromise (BEC) in which the scammers or cyber criminals pose as executives, vendors or trusted business associates to trick or lure victims into dispensing huge sums of money or sharing sensitive information.
3. **Ransom-ware:** -Exists in forms of Malware otherwise referred to as malicious software, viruses, worms, Trojans, spyware. These penetrate a system usually via a link on an unwanted software download that encrypts data, by either taking over the operating, collects sensitive data, manipulates and blocks access to network components or may destroy the stored data or shut down the system completely. The intruders would normally demand payment for release of their control of the hacked system.
4. **Denial of service (DOS) attacks:** This entails overwhelming or overtaking of online services by cybercriminals with more sophisticated technology thereby, rendering them inaccessible to the original owners.
5. Insider threats such as staff and students uncontrolled or uninformed behaviour through the use of unsecured networks and devices. These actions may result to damage or corruption of the systems that may result in financial losses.
6. Online harassment and cyber bulling occur when legitimate operators are unnecessarily bullied or threated by cybercriminals for the purpose of making money. (Liz, 2021)

Importance of cyber security in education

The benefits or importance of cyber security in education has been summarised by Sophos, (2021) Thus:

- Protection of sensitive student and staff data thereby improving student and staff protection. Every student and staff in an educational institution has peculiarities that are personal and need to be protected from the glare of the public. It is by so doing that staff

and students will feel protected and would go about their duties without fear of intrusion or intimidation from the public.

- Prevention of disruptions to academic operations thus enhancing academic integrity. When data of educational institutions are protected from public intrusion, the academic programmes run smoothly without disruptions leading to timely completion of studies by student which most often result to the evolution of high integrity for such schools attracting high patronage from the public.
- Safeguarding of intellectual property and research, thereby ensuring increased efficiency and productivity. If the research findings and other intellectual holdings of the schools are protected and preserved, current and future operations of the schools would be enhanced leading gradually but steadily to efficiency and optimum productivity.
- Compliance with standard organisations' regulations. Different quality assurance outfits are engaged in monitoring operations of institutions by the enactment of appropriate guidelines for standard operations. When the operations of the institutions are recorded over the years for reference, there would be deliberate attempts to adhere to the stipulations of the established standards.
- Support for digital transformation and innovation with increased confidence in digital platforms. When educational data are stored in the cloud, there are hardly any chances of damage or falsification of same, authenticity of such data over a reasonable period of time is assured. This builds confidence in the operators who in turn support digital information storage.
- Protection of educational technology investments. Educational technology equipment and infrastructure are capital intensive and require adequate care and maintenance for them to serve their usefulness over time.

- Improved incident response and recovery from cyber threats. In the course of handling cybercrime threats, lessons are learnt and worthy experiences gained such that there are improvements in the handling of reoccurrence of threats subsequently.
- Maintenance of institutional reputation and trust. Institutions that have recorded high resistance to cyber threats over a period of time gradually build a favourable reputation for themselves and thus attract public trust, admiration and patronage.

Consequences of neglecting cyber security in education

Any educational institution that play prangs with cyber security is open to some of these risks as enunciated by Griffiths and Kuss (2015).

1) Financial losses and reputational damage. There is no gainsaying the fact that institutions that play kids gloves with cyber security stand the risks of not only experiencing heavy financial losses but also serious smear on their reputation and public acceptance.
2) Compromised student and staff safety and wellbeing. All persons engaged in educational institutions that do not take cyber security seriously stand the risks of being exposed to various forms of embarrassment, harassment including the safety of their lives and properties.
3) Disrupted academic operations and other progammes are common features in educational institutions that tow with cyber security.
4) Educational institutions that do not have elaborate arrangements for effective and efficient cyber security outfits are prone to loss of intellectual property and research findings.
5) Regulatory non-compliance to set standards by educational institutions often result to penalties either in forms of imposition of fines or outright suspension from operations for stipulated periods.
6) Decreased trust among students, parents and other relevant stakeholders is often experienced by schools that do not have established frameworks for cyber security.
7) In addition institutions that neglect cyber security are more likely to be faced with increased risk of cyber-attacks and data breaches of their networks.

8) Long-term damage to institutional reputation and credibility are sure aftermaths of either total or partial disregard to cyber security measures by educational institutions, (Ponemon Institution, 2020).

Cyber security best practices for educational institutions

Educational institutions can avert the aforementioned consequences of neglecting cyber security by adopting some of the under listed measures in key aspects of cyber security in Education viz:

i. **Network Security: -** This involves protecting educational networks from unauthorised access, malwares and other threats. It includes firewalls, Infusion Detection/Prevention Systems (IDS/IPS) and virtual Private Network (VPNs).
ii. **Data Protection:** Safeguarding sensitive student and staff data, including: encryption, access controls, backup and recovery systems and data loss prevention (DLP) tools.
iii. **End Point Security:** Is concerned with securing devices connected to the network such as laptops, desktops, mobile devices and Internet of Things (IOT) devices.
iv. **Identity and Access Management (IAM): -** This entails managing user identities and access to educational resources with regards to authentication, authorisation Single Sign–On (SSO) and multi-Factor Authentication (MFA).
v. **Incident Response:** This takes care of preparing for and responding to cyber security incidents through incident response plans, threat detection and analysis, containment and eradication and recovery and post-incident activities.
vi. **Security Awareness and Training:** Engaging in educating students, staff and faculty on cyber security best practices such as phishing simulations, security awareness campaign, training programmes and cyber security workshops.
vii. **Cloud Security:** Involves protecting educational data and applications in cloud environments to include Cloud Access Security Brokers (CASBs), cloud security gateways and encryption.

viii. **Compliance and Regulations:** Meeting regulatory requirements for educational institutions such as Family Educational Rights and Privacy Act (FERPA), General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCIDSS).

ix. **Threat Intelligence:** Takes care of monitoring and analysing potential threats such as threat intelligence feeds, vulnerability management, and penetration testing and risk assessments.

x. **Cybersecurity Governance:** This involves establishing policies, procedures and oversight through cyber security policies, risk management frameworks, compliance frameworks and incident response planning strategies (Stealthlab, 2021).

According to the Federal Bureau on Intelligence FBI (2021), the under listed key aspects help educational institutions protect against cyber threats and ensure a secure learning environment. The institutions may adopt some of the following specific activities.

- Conducting Regular Security audits and risk assessments by identifying vulnerabilities and addressing same.
- Implementing robust cyber security policies and procedures.
- Providing cyber security training for students and staff on cyber security best practices.
- Investing in advanced security technologies such as artificial Intelligence (AI) solutions.
- Fostering a culture of cyber security awareness.
- Establishing incident response plans, teams and procedures for responding promptly to security incidents.
- Monitor and analyse network activities.
- Collaborate with cyber security experts and peers.
- Using secure cloud services by choosing reputable cloud providers with robust security measures.

- Complying with data protection regulations by adhering to relevant laws and regulations such as General Data Protection Regulation (GDPR), Children's Online Privacy Protection Act (COPPA) and Family Educational Rights and Privacy Act (FERPA).

Conclusion

By prioritising cyber security, educational institutions can protect their students, staff and reputation, while ensuring a secure and supportive learning environment for all that will lead to optimum productivity in the education industry in Nigeria.

References

Bryan, C. (2024). *The Impact of Security Breaches on Educational Institutions Chichester*: John Wiley, PP. 384 – 466.

Chancey, T. (2023). Cyber Security in Schools

FBI (2021). *Increasing cybercrime since the pandemic concerns for psychiatry*. https://linkspinger.com/article/101007/511920-021-01228w.

Griffiths, M and Kuss, D. (2015). *Online additions, gambling, video gaming and social networking, the handbook of the psychology of communication Technology, Chicester*: John Wiley. Pp384-466.

Liz, S. (2023). *Impact of Cyber Security, threat hot cyber security Technologies.* Cyber Security Research Organization.

Mikhail, K. (2023). *Core tips for data security in Educational Institutions.*.

National Bureau of Statistics (2024). *Report on primary education*.

Ponemon Institution (2020). *Cost of a data breach report*. https//www/ibm.com/security//digital-assets/cost-data-breach-report/

Sopho, S. (2021). *The State of ransom ware.* https//secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-ofransomeware-2021-wp-pdf.

Stealthlab, O. (2021). *Cyber Security in Education and Research Institutions*. https//www.stealthlabs.com//industries/education.research-institutions.

U.S. Department of Education.(2020). *Protecting student privacy.* Https/studentprivacy.ed