Region - Educational Research and Reviews, 2023, Volume5, Issue6
DOI: 10.32629/rerr.v5i6.1450
ISSN Online: 2661-4634
ISSN Print: 2661-4626

Strengthening the digital learning environment: integrating cybersecurity risk management and data protection methodologies

Longe OLUMIDE[1], Talabi ADEDOYIN[2,*]

1. Faculty of Computational Sciences and Informatics, Academic City University College, Accra AD 421, Ghana
2. African Centre of Excellence in Technology Enhanced Learning, National Open University of Nigeria, Abuja 900001, Nigeria
Corresponding author.
Email address: doyin.talabi@gmail.com

Abstract: Digital learning refers to the use of technology in learning that involves the use of at least a piece of technology like a laptop. The adoption of digital technologies and resultant transformation of organizations were accelerated in part by COVID-19 pandemic but have attracted cybersecurity criminals and hackers who want to gain unauthorized access to personal data, sensitive personal data like financial and health information to commit fraud or cybercrime.

The objective of the paper is to raise awareness for active cybersecurity risk management and data privacy compliance, especially in educational institutions. An online questionnaire was developed and distributed using Google Forms, having questions related to cybersecurity and data protection methodologies with a sample size of 100 participants. The results from the survey underscored the importance of having controls and policies to prevent cyberattacks and data breaches.

The paper concluded that it is very important to create awareness among stakeholders and implement cybersecurity controls and utilize data protection methodologies to protect personal data and corporate information. This would ensure compliance with related regulations and laws.

Key words: awareness; compliance; data privacy; digital learning; educational institutions; hackers; personal data

1 Introduction

Digital learning refers to the use of technology in learning (and teaching). This can be a face-to-face lecture, seminar or webinar that involves the use of at least a piece of technology like a laptop, desktop or mobile phone (twinkl.com, 2023). This framework has been adopted by many educational institutions in delivering content to their students. This adoption of digital technologies and resultant transformation of organizations were accelerated in part by COVID-19 pandemic, which caused global economic shutdown, stoppage of physical movement with varying consequences and impact on social life and provision of educational services [1].

This exponential increase in the use of digital learning platforms and technologies attracted cybersecurity criminals and hackers who want to gain unauthorized access to personal data, sensitive personal data like financial and health information for use to commit fraud and other forms of cybercrime. For these reasons, proactive cybersecurity

management and data protection issues have become of concern in the cyberspace in general and in the digital learning space in particular.

Many countries including Nigeria, Ghana, South Africa and the European Union have enacted *Data Privacy and Protection Regulations* to guide personal data management practices in their jurisdiction. Ghana promulgated its *Data Protection Act* in 2012 [2]. The European Union promulgated its *General Data Protection Regulation* (GDPR) effective in May 2018. South Africa created *Protection of Personal Information Act* (POPIA) effective in 2021, though it was promulgated in 2013 [3]. And the *Nigeria Data Protection Act* was signed into law on June 12, 2023 [4]. In all the privacy regulations, there are similar provisions for protecting data, list of legal bases for processing personal data, rights of data subjects (owners), obligations of data controllers and fines for infractions.

In the US, *The Family Educational Rights and Privacy Act* (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) protects the privacy of student education records and it applies to all schools that receive funds from U.S. Department of Education. FERPA gives certain rights to parents until the child is 18 or has gone beyond high school education. Parents or students of age have the right to inspect and review educational records kept, have right to correct records and the schools need written permission to disclose information [5].

The aim of the paper is to protect the personal data and information carried by educational institutions and the objective is to raise awareness of active cybersecurity risk management and protecting the privacy and confidentiality of personal data by highlighting controls, policies and practices that should be in place to secure the digital learning space for all stakeholders.

2 Materials and methods

An online questionnaire was developed to conduct a survey using Google Forms and circulated to different online platforms on December 15, 2023. The questionnaire had sections for collecting participant information, enquiring about awareness and understanding, current practices, user experience, effectiveness and improvement, feedback and reporting, overall satisfaction and any additional comments that the respondents may have. The age of participants engaged in the evaluation range from 18 to 55 years and above.

The sample size consisted of 100 people, male and female with different roles in education including students, teachers, administrators, parents, management consultants, retirees and IT professionals. Frequency distributions was used to describe the responses to the questions and a mixed method approach was used in the overall data interpretation since the questionnaire contained some open comments and Likert scales.

For ethical considerations, the questionnaire had an introduction which explained the purpose of the questionnaire that it is for research only and that the personal data given will kept confidential and participants are free to withdraw from participating at any time.

3 Results

The results from the administration of the online questionnaire showed that 80% of respondents were male and 20% female. 38% were aged between 45 and 54, 32% aged 55 and older, 18% between 35 and 44, 10% were aged between 25 to 34 and 2% aged between 18 and 24. 43% were IT professionals, 15% were teachers, 12% were administrators, and 8% were students, Business men, parents, management consultants, bankers, lawyers, accountants, retirees constituted the balance. 52.6% have been involved in digital learning environments for more than 10 years, 30.9% for between 6 and 10 years, 11.3% for between 3 and 5 years, 4.1% for 1 to 2 years and 1% for less than 1 year. 38.4% are extremely familiar with the concept of cybersecurity in digital learning environments, 30.3% moderately familiar, 18.2% slightly familiar,

10.1% extremely familiar and 3% not familiar. 69% of respondents are aware of cybersecurity incidents or data breaches that have occurred in digital learning environments, while 31% were not.

88% agree that the integration of cybersecurity and data protection methodologies is essential for the digital learning environment, 10% strongly disagree and 2% are neutral. 44% perceive that the level of integration of cybersecurity risk management in their digital learning environment is moderately integrated, 30% say they are slightly integrated, 16% say very integrated, 3% feel that it is extremely integrated while 7% say it is not integrated. 61% have received training or guidance on cybersecurity best practices within the digital learning environment while 39% have not. 40.4% believe data protection methodologies are moderately implemented in their digital learning environment, 39.4% believe they are partially implemented, 19.2% say they are fully implemented and 1% say data protection methodologies are not implemented at all.

38.4% are moderately confident in the security of their personal data when using digital learning platforms, 28.3% are very confident, 21.2% are slightly confident, 6.1% are extremely confident while the balance 6.1% are not confident at all about the security of their personal data. 58% say they have encountered security-related challenges or issues while using digital learning platforms and 42% say they have not. 45% say that the current cybersecurity measures in their digital learning environment are moderately effective, 27% slightly effective, 25% very effective and 3% say the cybersecurity measures are extremely effective.

51% are comfortable with providing feedback or reporting security concerns within the digital learning environment, 20% feel moderately comfortable, 12% slightly comfortable, 11% extremely comfortable and 6% are not comfortable at all. 99% believe that user feedback plays a role in shaping the cybersecurity policies of digital learning platforms and 1% does not. 99% will be more inclined to use a digital learning platform that actively communicates and emphasizes strong cybersecurity and data protection measures, while 1% will not. On a scale of 1 to 10, 22% are not satisfied at all with the overall security and data protection features of their current digital learning environment. 18% are averagely satisfied, 30% slightly satisfied and another 30% very satisfied.

The following were suggested as improvements or additional measures that could enhance the cybersecurity and data protection of digital learning environments. First, enhance laboratory experience, knowledge transfer, and increase consumer awareness of network and privacy security in digital learning environments. This could include a quick security training tailored to the environment before usage. Second, create platforms for affordable training and deploy enhanced technology. Cybersecurity should be integrated from system design stage; More training and auditing should be conducted and blockchain technology should be used in the development of eLearning platforms; Measures should be put in place to prevent data breaches and secure intelligent algorithm integrated with multi-level access systems in place. Two-factor authentication should be used and periodic phishing testing should be undertaken.

There should be policies on reporting any perceived cyber/data security breach, investments in modern IT infrastructure and more expert involvement. Decision makers in the environment should be properly informed about the importance of cybersecurity and data protection as this will be more effective if they take the lead.

The respondents made additional comments and suggestions regarding the integration of cybersecurity and data protection methodologies in digital learning environments. The suggestions include that cyber security and data protection methodologies should be the business of everyone involved in the digital learning environment. The regulators of cybersecurity and data protection should collaborate to raise awareness, create laws and enforce the laws. Cybersecurity and data protection methodologies should work in tandem to provide greater assurance that transactions are securely and safely conducted over the Internet. Digital learning platform users need to be trained against social engineering attacks

which could compromise the most advanced installed cybersecurity technical defense mechanisms. Developers need to understand the implications of data breaches in digital learning environments.

4 Discussion

Majority of the respondents are stakeholders in educational sector and half of the respondents have been involved with digital learning environments for more than 10 years. Many of the respondents are familiar with the concept of cybersecurity in digital learning environments. This suggests that the respondents know the importance of cybersecurity and data protection in securing the digital learning landscape, which makes their responses credible.

Slightly over half have encountered security-related challenges or issues while using digital learning platforms. Majority of the respondents are aware of cybersecurity incidents or data breaches that have occurred in digital learning environments and a greater majority of respondents agree that the integration of cybersecurity and data protection methodologies is essential for the digital learning environment. This confirms that cyberattacks and data breaches occur and it is important to implement cybersecurity controls and utilize data protection methodologies to protect personal data and corporate information of users. It is also critical to create cybersecurity awareness among stakeholders.

Nearly all the respondents are more inclined to use a digital learning platform that actively communicates and emphasizes strong cybersecurity and data protection measures. This confirms that having necessary controls in place will encourage wide usage by stakeholders including students, teachers and administrators.

In the digital learning space, a lot of activities take place that involve the collection and processing of personal data connecting through both private and public networks, which may not be secure and can create exposure to cyberattacks and data theft. The records used and shared include admission lists, academic records, financial records, employment records, medical records, administrative records, online courses etc. The stakeholders that may have access to these personal data include authorized employees, teachers, vendors, other employees and the students themselves [7].

According to global report by stastisitca.com, 740 million [6] pupils were enrolled in primary schools in 2020 as against 650 million in the year 2000. For secondary school children, there were 452 million students in secondary schools in the year 2000 and 614 million [7] in 2020. The number of students in higher education institutions increases from 100 million in 2000 to about 220 million in 2020 [8]. This gives a total of 1.574 billion potential accounts that can be hacked or compromised as many educational institutions are transforming to digital learning platforms. The educational sector was the most targeted by malware attacks between July and August 2022, with about 5.13 million attacks within 30 days [9]. Microsoft reported that the education sector is the most vulnerable sector to malware threats, accounting for more than 68% of reported threats (terranovasecurity.com, 2023) [10]. According to IT security guru (itsecurityguru.com, 2023), 5. 23 million educational records have been hacked in 2023, up from 1.19 million records in 2022.

Individuals and educational institutions are also connected to social media platforms like LinkedIn and Facebook, as well as third party online educational course providers such as Coursera and Google. All these have implication for cybersecurity management and data protection [11]. So, when technology tools and applications are used during the teaching and/or the learning process, there is a high probability for unauthorized access, hacking collection and/ or storage of personal data without the explicit consent of the (data subject) owner.

Many collaborations with third party online education content providers to enrich curriculum content were done without adequate diligence about whether the provider is data privacy compliant, resulting in possible exposure of personal data to unauthorized users and leakage on the internet with dire consequences. Educational institutions have a duty to protect their students from exposures to radical groups and ideas, as well as online harassment and cyber bullying [12]. Therefore, it is very important to monitor and control online environments for privacy and safe usage.

The respondents to the questionnaire recommended cybersecurity risk management approaches that can be used. These include increased awareness for digital learning environment consumers on cyber and privacy security, implementation of block chain technology in the development of eLearning platforms, use of multi-level access systems and everyone should be security conscious from the system design stage. Two factor authentication should be used for data authentication and practical learning provided with periodic phishing testing.

For data privacy and protection compliance, the various data protection regulations like the *EU General Data Protection Regulation* (GDPR) [13] and the *Nigeria Data Protection Act 2023* [14] lay out the roles, responsibilities of data controllers (organizations that process personal data), rights of data subjects (owners of data owners) and sanctions for non-compliance. Also, in the US, educational institutions must comply with the *Family Educational Rights and Privacy Act* (FERPA).

5 Conclusion

Digital learning platforms have become a de-facto standard for teaching and learning. To guarantee safety of the digital learning space, educational institutions and content providers must put in place adequate cybersecurity measures supplemented with data protection methodologies for security, confidentiality and integrity in order to protect digital assets (dporganizer,2022) [15]. In particular, educational institutions should put in place data protection practices and methodologies should put in place to ensure compliance with data protection and related regulations [16]. These would include obtaining formal consent from students, parents and guardians when collecting and using personal data. Also, they must state clearly the purposes of the data collected and how the data will be used.

Educational institutions must provide infrastructure and resource for cybersecurity and data privacy compliance. They must thoroughly vet third vendors and applications for security and compliance before connecting to such applications or resources. Educational institutions must have data privacy notices in their locations, develop other related policies like the data protection policy and data retention policy. These policies establish how academic records are stored, processed and kept. Finally, the need for continuous cybersecurity and data privacy compliance awareness workshops is important as the digital safety landscape continue to evolve.

Conflicts of interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Twinkl. (n.d.). Digital learning. *Twinkl Teaching Wiki*. https://www.twinkl.com.ng/teaching-wiki/digital-learning

[2] Ghana Data Protection Commission. 2012. *Data Protection Act [Act 843]*. https://www.dataprotection.org.gh/

[3] Lucarini F. 2023. GDPR vs. POPIA: comparison of main similarities and differences. *Advisera*. https://www.advisera.com/gdpr-vs-popia/

[4] National Digital Policy Commission. 2023. *Nigeria Data Protection Act 2023*. [Nigeria Data Protection Commission]. https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf

[5] U.S. Department of Education. (n.d.). *Family Educational Rights and Privacy Act (FERPA)*. [U.S. Department of Education]. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[6] Statista.com. 2022. Number of pupils in primary education worldwide. https://www.statista.com/statistics/1227106/number-of-pupils-in-primary-education-worldwide/

[7] Statista.com. 2022. Number of pupils in secondary education worldwide. https://www.statista.com/statistics/1227098/number-of-pupils-in-secondary-education-worldwide/

[8] World Bank. 2021. Tertiary education. World Bank. https://www.worldbank.org/en/topic/tertiaryeducation#:~:text=Today there are around 220, from 100million in 2000:

[9] Statista.com. 2022. Industry sectors targeted by malware attacks worldwide. https://www.statista.com/statistics/1326618/industry-sectors-targeted-by-malware-attacks-worldwide/:

[10] Terranova Security. (n.d.). Cyber Security and Going Back to School. *Terranova Security*. https://terranovasecurity.com/blog/cyber-security-and-going-back-to-school/:

[11] Hoel T, Chen W. 2018. Privacy and data protection in learning analytics should be motivated by an educational Maxim--towards a proposal. *RPTEL*, 13(1): 20. https://doi.org/10.1186/s41039-018-0086-8: https://doi.org/10.1186/s41039-018-0086-8

[12] Bates T, Bates A. 2019. Teaching in a digital age. *BCcampus Open Education*. https://opentextbc.ca/teachinginadigitalage/chapter/9-9-the-sections-model-speed-and-security/:

[13] GDPR Info. 2018. *General Data Protection Regulation (GDPR).* [GDPR info].https://gdpr-info.eu/:

[14] National Digital Policy Commission. 2023. [National Digital Policy Commission]. https://ndpc.gov.ng/:

[15] DPOrganizer. (n.d.). Technical and Organisational Measures. [DPOrganizer]. https://www.dporganizer.com/blog/privacy-management/technical-organisational-measures/:

[16] Yusuf T. 2020. Privacy and data protection in the nigerian educational sector. *Africa Academic Network on Internet policy*. https://aanoip.org/privacy-and-data-protection-in-the-nigerian-educational-sector/#