Cyber Security in the Era of Digitalization: Implications for Educational Management

By

Innocent Chiawa Igbokwe, PhD
Department of Educational Management
Nnamdi Azikiwe Univeristy, Awka
(ic.igbokwe@unizik.edu.ng)

Abstract
As educational institutions embrace digital transformation, the integration of technology in educational management has introduced both opportunities and challenges. One of the most pressing challenges is ensuring cyber security. This research paper explores the implications of cyber security in educational management amidst the era of digitalization. The paper discusses the various cyber threats faced by educational institutions, the impact of these threats on educational management, the strategies that can be employed to enhance cyber security and other best practices to mitigate risks.

Keywords: Cyber security, Cyber threat, Digitalization, Educational Management, etc

Introduction

The digital era has revolutionized many sectors, including education. The rise of digitalization in education has facilitated improved access to educational resources, enhanced communication between educators and students, and streamlined administrative processes. As has been argued by Garrison and Vaughan (2013), tools such as learning management systems (LMS), online libraries, and digital collaboration platforms have transformed the educational landscape. This is the logic of digital transformation. Yamba and Abwino (2023) define digital transformation as the process of adoption and implementation of digital technology by school organizations in order to create new or modify existing products, services and operations into translating learning processes into digital formats Digital tools and platforms have enhanced teaching, learning, and administrative processes in educational institutions. Then, the digitalization of education can radically change the essence of education as a space of communication, dialogue, socialization, forming not only knowledge but social skills as well (Baeva & Grigorev, 2020).

Meanwhile, the integration of digital technologies into educational processes has transformed the way knowledge is imparted and acquired. From online learning platforms to administrative systems, educational institutions have embraced digitalization to enhance efficiency, accessibility, and collaboration. However, this digital transformation also brings significant risks in the form of cyber threats. Educational institutions are increasingly becoming targets for cyber-attacks due to the vast amounts of sensitive data they handle. This cyber threat come in different ways such as malware, ransomware, and phishing attacks, posing serious risks to data security and operational continuity. It is actually risk to be ignorant of such cyber threats and attacks (Adorjan, & Ricciardelli, 2019). This calls global attention to cyber-security.

Cybersecurity can also be defined as the activity, process, ability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation (DHS., 2014). Yamba and Abwino (2023) cited the Cyber Security and Cyber Crimes Act, 2021 of the Zambian laws which comprehensive defines cyber security concerns tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment, organization and user assets. Cyber-crime or cyber-attack is seriously dangerous. Some places in our educational environment are more prone to cyber-attacks. Irons and Crick (2022) identified a number of points in educational systems that could potentially be vulnerabilities for attackers to exploit, including, but not limited to: Hardware and infrastructure; Software and integrated systems; Connected university systems (e.g. finance, HR, etc); Virtual learning environments; Email, instant messaging, and connections to social networking; Data storage (both personal and academic); and Users. Each of these vulnerabilities platform can be complex and

dangerous. Baeva and Grigorev (2020) maintains that the most dangerous threats may be those caused by targeted cyber-attacks and cyber terrorism, which may concern not only gaining access to sensitive information, disseminating fake information, but also cyber bullying and cyber fraud in various forms (including social networks used for educational process and insecure online services).

Cyber Threats in Educational Institutions

Cyber threats are real and varied. For Irons and Crick (2022), cyber-attacks can come from a variety of different sources, with the nature of the attack and the attack vector varying depending on the attack type. Despite the benefits, digitalization has exposed educational institutions to various cyber threats, including data breaches, ransomware attacks, phishing, and Distributed Denial of Service (DDoS) attacks (Shafiq & Gu, 2019). These threats pose significant risks to the confidentiality, integrity, and availability of educational data and services. Some of the cyber threats faced by educational institutions include:

Data Breaches

Data breaches involve unauthorized access to sensitive information. Educational institutions hold vast amounts of personal data, including student records, financial information, and research data, making them prime targets for cybercriminals (Choi & Lee, 2020; Ponemon Institute, 2021). Schools and universities store vast amounts of personal and financial information, making them prime targets for cyber criminals (McGettrick, 2013). Data breaches involving academic records can compromise the fairness and credibility of educational processes (Mitchell, 2020). Data breaches can have severe consequences, including financial losses, legal liabilities, and reputational damage. For instance, research data, particularly from high-profile projects or sensitive areas of study, can be targeted by cybercriminals or competitors. Breaches involving research data can undermine academic innovation and intellectual property (Olavsrud, 2020). The breaches can lead to identity theft, financial loss, and legal consequences. In 2022, the Los Angeles Unified School District faced a ransomware attack that disrupted its IT systems and compromised sensitive data. The attack led to the temporary shutdown of the district's online systems and raised concerns about the vulnerability of educational institutions to cyber threats (Green, 2022).

Ransomware Attacks

Another significant security threat facing schools is ransomware attacks. Someone like Kshetri, (2021) argued that ransomware attacks can cripple educational institutions by encrypting critical data and demanding a ransom for its release. Such attacks can disrupt educational processes and lead to significant financial loss. Ransomware is malicious software that encrypts files or locks users out of their systems until a ransom is paid (Shin, 2018). Schools are attractive targets for ransomware attacks due to their reliance on digital systems for administrative tasks and the potential for financial gain from ransom payments. A successful ransomware attack can disrupt school operations, compromise sensitive data, and incur significant financial losses.

Ransomware attacks encrypt an institution's data and demand a ransom for its release. Such attacks can cripple educational operations and result in significant financial losses (Alotaibi & Almagwashi, 2021). For instance, in 2020, University of California, San Francisco ransomware attack where the attackers demanded for ransom (BBC News, 2020). Again, this incident highlights the severe impact of ransomware attacks on educational institutions and the importance of robust cyber security measures.

Phishing Attacks

One prevalent type of security attack on schools is phishing. Phishing attacks are prevalent in educational settings, where attackers use deceptive emails to trick users into revealing confidential information (Jensen, Dinger, Wright, & Thatcher, 2017). Phishing attacks involve the use of deceptive emails, messages, or websites to trick individuals into divulging sensitive information such as login credentials or financial data (Ferrante & Rowe, 2020). School staff, students, and parents may receive phishing emails disguised as official communications from the school administration, leading to compromised accounts or unauthorized access to sensitive systems.

Phishing attacks use deceptive emails or messages to trick individuals into disclosing sensitive information or downloading malware. These attacks can compromise personal and institutional data

(Shafiq & Gu, 2019). According to San Diego Unified School District (2018) records, the institution experienced a cyber breach caused by a phishing attack that compromised employee login credentials. This case underscores the dangers of phishing attacks in educational institutions.

Distributed Denial of Service (DDoS) Attacks

More so, Distributed Denial-of-Service (DDoS) attacks pose a threat to schools' digital infrastructure. DDoS attacks involve flooding a network or website with an overwhelming amount of traffic, causing it to become unavailable to legitimate users (Shin, 2018). Schools' websites or online learning platforms may be targeted by DDoS attacks, disrupting access to educational resources and communication channels. These attacks can disrupt online learning and administrative processes (Choi & Lee, 2020). This kind of attack to can overwhelm an institution's network with traffic, making online services unavailable to users.

Insider Threats

Cyber-attacks usually come from multiple sources but one of the most dangerous is the one that comes from the inside. The school data can be compromised by the operators or those involved in the school in one way or the other. Insider threats involve malicious actions by individuals within the institution, such as employees or students, who misuse their access to sensitive data and systems (Kim & Solomon, 2022). This is why Willison and Warkentin, (2013) opined that students, faculty, and staff may inadvertently or maliciously cause security breaches, highlighting the need for robust internal controls and training.

Implications of Cyber Threats for Educational Management

There are several implications of cyber threat and attacks for educational management. Some of these implication are:

- **Disruption of Educational Services.** Cyber attacks can disrupt the delivery of educational services, causing significant downtime and hindering access to digital learning platforms (Shafiq & Gu, 2019). Such disruptions can hinder the institution's ability to deliver quality education (Olavsrud, 2020). This disruption can adversely affect the learning experience and institutional operations. This kind of disruption to stop ongoing online classroom or block access to admission and enrolment.
- **Financial Losses.** Cyber-attacks can result in substantial financial losses due to ransom payments, data recovery costs, legal fees, and fines for non-compliance with data protection regulations (Choi & Lee, 2020). In 2020, University of California, San Francisco experienced a ransomware attack that encrypted several servers in its School of Medicine. The attackers demanded a ransom of $1.14 million, which the university paid to regain access to its data (BBC News, 2020). Cyber threat can lead to significant financial losses.
- **Damage to Reputation.** Data breaches and other cyber incidents can damage an institution's reputation, leading to loss of trust among students, parents, and stakeholders (Alotaibi & Almagwashi, 2021). Loss of trust among students, parents, staff, and the public can lead to decreased enrollment, loss of funding, and long-term reputational harm (Mitchell, 2020). In 2014, the University of Maryland experienced a significant data breach that exposed the personal information of over 300,000 individuals. The breach involved names, Social Security numbers, dates of birth, and university identification numbers. The incident highlighted the need for enhanced security measures and better data encryption practices (Kirk, 2014). This loss of trust can have long-term repercussions on student enrollment and funding.
- **Legal and Regulatory Consequences.** Educational institutions are required to comply with various data protection and privacy regulations. Failure to protect sensitive data can result in legal penalties and regulatory fines (Kim & Solomon, 2022). An educational institution can be sued for violation of privacy even when it is not their fault and so, effort must be made by institutions of learning to invest in cybersecurity.
- **Impact on Stakeholder Trust.** Cyber incidents can erode the trust of students, parents, faculty, and other stakeholders. Ensuring robust cyber security measures is essential to maintaining stakeholder confidence (Choi & Lee, 2020). In 2018, the San Diego Unified School District

reported a data breach that exposed the personal information of over 500,000 students and staff members (San Diego Unified School District, 2018). It is factual, Baeva and Grigorev (2020) contend that threats to personal security may be associated with a violation of human rights in digital environment, including copyright, honor and dignity, confidentiality etc.

Strategies for Enhancing Cyber Security in Educational Management

Incorporating advanced strategies and technological best practices is crucial for enhancing cyber security posture and mitigating risks in educational management. Some of these strategies are;

1. **Implementing Strong Authentication Measures.** Strong authentication measures, such as multi-factor authentication (MFA), can significantly reduce the risk of unauthorized access to sensitive data and systems (National Institute of Standards and Technology [NIST], 2020).
2. **Implementing a robust incident response framework.** This type of security posture enables timely detection, containment, and recovery from security incidents, minimizing disruption to educational operations. Similarly, adopting a defense-in-depth approach, which involves layering security controls across networks, endpoints, and applications, provides multiple layers of defense against evolving cyber threats (Smith & Jones, 2021).
3. **Apply the principle of least privilege.** This principle calls for only enabling access to the online classroom when it is required, for specific roles and activities, and only for those academics and learners who need access when the access is actually needed. For Irons and Crick (2022), least privilege also means that access should be removed when access to the online classroom is not required and related to this principle of least privilege, ensure there is an end of life plan to manage access when students and staff leave (progression, graduation, or otherwise), managing student records and ensuring that obsolete and unprotected equipment is decommissioned and removed; and Constant vigilance (and do not be afraid to question).
4. **Regular Security Training and Awareness Programs.** Educating students, faculty, and staff about cyber security best practices is crucial. Regular training sessions can help raise awareness of common threats, such as phishing and social engineering attacks, and promote safe online behaviors (Shafiq & Gu, 2019). Indeed, all participants in the educational learning environment, academic staff, professional services staff and students, should be aware of the increasing need for robust and adaptable cybersecurity in the classroom (Irons & Crick, 2022).
5. **Developing Incident Response Plans.** Having a well-defined incident response plan enables institutions to respond quickly and effectively to cyber incidents, minimizing damage and restoring normal operations (NIST, 2020). This may be in form of developing continuous monitoring and threat intelligence analysis enable proactive threat detection and mitigation, allowing educational institutions to stay ahead of cyber adversaries and protect their systems and data effectively (Johnson, 2019).
6. **Utilizing Encryption.** Encryption protects sensitive data by converting it into a format that can only be read by authorized individuals. Implementing encryption for data at rest and in transit is crucial for maintaining data security (Kshetri, 2021; Kim & Solomon, 2022).
7. **Regularly Updating and Patching Systems.** Keeping software and systems up to date with the latest security patches helps protect against known vulnerabilities that could be exploited by attackers (Alotaibi & Almagwashi, 2021).
8. **Conducting Vulnerability Assessments and Penetration Testing.** Regular vulnerability assessments and penetration testing help identify and address security weaknesses before they can be exploited by attackers (Shafiq & Gu, 2019). Regular risk assessments and security audits help to discover areas of vulnerabilities and of efforts are seriously made to strengthen the entire security architecture of educational institutions.
9. **Establishing Access Controls.** Implementing strict access controls ensures that only authorized individuals have access to sensitive data and systems. This reduces the risk of insider threats and unauthorized access (Choi & Lee, 2020).
10. **Establishing comprehensive security policies and procedures.** Promulgation of security policies and procedure is essential for promoting a culture of security and compliance within the organization. According to United States Department of Education (2020), this includes implementing data protection protocols, incident response plans, and access controls to safeguard sensitive information and mitigate the impact of security incidents.

11. **Collaboration and information sharing among educational institutions.** Building networking of intelligent security information sharing platform among schools, collaborative partners, education ministries and government agencies can also enhance cyber security resilience. By exchanging threat intelligence, best practices, and resources, institutions can collectively strengthen their defenses and respond more effectively to emerging cyber threats (National Institute of Standards and Technology, 2018).
12. **Understanding of relevant threat actors and their capabilities.** Conscientization of relevant stakeholders of educational institutions on the significant threat actors and their capabilities. It is an approach that is needed to detect the ever growing complex dimensional tactics of the threat actors (Boehm, Curcio, Merrath, Shenton, & Stähle, 2020). This will help to define the institutional threat landscape- the tactics, techniques, and procedures they use to exploit enterprise security – by understanding its specific threat.
13. **Prioritization of cybersecurity reporting.** Every educational institution must be able to open their doors for cybersecurity reporting. Cybersecurity reporting unites are to be created and headed by cybersecurity experts. Their reports must be able to show top risks, key assets, recent incidents, counter risk measures, implementation accountability, the institution's resilience in the face of cyber threats and so on (Kaplan, Richter, & Ware, 2020). The reports have to provide technical information for management decision making.
14. **Popularization of cybersecurity education and curriculum.** There is need to inculcate cybersecurity education in the mind of the stakeholders of education. That is to educate the users of technology on the potential risks they face when using internet communication tools, such as social media, chat, online gaming, email and instant messaging (Rahman, Sairi, Zizi & Khalid, 2020). Policy makers should also try to update and prepare adequate cybersecurity curriculum that can be used by teachers at all levels of education to create awareness in the learners.

Conclusion

Cyber security is an emerging aspect of educational management in the digital era. It is the duty of everyone in an educational institution to stay safe online. Educational institutions must make adequate investment for cyber security and implement comprehensive cyber security strategies to protect sensitive data, ensure the continuity of educational services, and maintain stakeholder trust. Consequently, through the adoption of best practices such as strong authentication measures, regular security training, and robust incident response plans, educational institutions can avoid landscape of cyber vulnerabilities, mitigate the risks associated with cyber threats and create a secure digital environment for learning and administration.

References

Adorjan, M. & Ricciardelli, R. (2019). Student perspectives towards school responses to cyberrisk and safety: the presumption of the prudent digital citizen, Learning, Media and Technology, 44(4), 430-442. https://doi.org/10.1080/17439884.2019.1583671.

Alotaibi, S., & Almagwashi, H. (2021). Cybersecurity awareness in educational institutions: Challenges and recommendations. *Journal of Information Security and Applications*, 58, 102825. https://doi.org/10.1016/j.jisa.2021.102825

Baeva, L & Grigorev A. (2020). Safety of digitalization of educational and social space. *Pakistan Journal of Distance & Online Learning, VI*(1), 231-246.

BBC News. (2020). University of California pays $1.14m ransom to hackers. Retrieved from https://www.bbc.com/news/technology-53214783

Boehm, J., Curcio, N., Merrath, P., Shenton, L. & Stähle, T. (2020). The risk-based approach to cybersecurity. In Cybersecurity in a Digital Era. *Digital McKinsey and Global Risk Practice*. http://www.mckinsey.com/

Choi, B., & Lee, I. (2020). The impact of information security threats on the educational sector. *Computers & Security*, 91, 101703. https://doi.org/10.1016/j.cose.2020.101703

DHS. (2014). A glossary of common cybersecurity terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. [Online]. Available: http://niccs.uscert.gov/glossary

Ferrante, A., & Rowe, M. (2020). A comprehensive look at the realities of phishing attacks and potential defenses. *Journal of Cybersecurity Education*, 4(1), 23-38.

Garrison, D. R., & Vaughan, N. D. (2013). *Blended learning in higher education: Framework, principles, and guidelines*. John Wiley & Sons.

Green, J. (2022). Los Angeles Unified School District hit by ransomware attack. *TechCrunch*. Retrieved from https://techcrunch.com/2022/09/07/los-angeles-unified-school-district-ransomware-attack/

Irons, A. & Crick, T. (2022). 'Cybersecurity in the digital classroom: Implications for emerging policy, pedagogy and practice'. In: B.A. Brown & A. Irons (eds.) *The Emerald handbook of higher education in a post-covid world: new approaches and technologies for teaching and learning*. Emerald, Bingley, pp. 231-244. https://doi.org/10.1108/978-1-80382-193-120221011

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, 34(2), 597-626.

Johnson, M. (2019). Cybersecurity in education: Risks and responsibilities. *Journal of Cybersecurity Education*, 3(2), 45-62.

Kaplan, J., Richter, W. & Ware, D. (2020). Cybersecurity: Linchpin of the digital enterprise. In Cybersecurity in a Digital Era. *Digital McKinsey and Global Risk Practice* http://www.mckinsey.com/

Kim, D., & Solomon, M. G. (2022). *Fundamentals of Information Systems Security* (4th ed.). Jones & Bartlett Learning.

Kirk, J. (2014). University of Maryland suffers massive data breach. *Computerworld*. Retrieved from https://www.computerworld.com/article/2487455/university-of-maryland-suffers-massive-data breach.html

Kshetri, N. (2021). Ransomware: Its evolution, socioeconomic factors, and policy implications. *Journal of Cyber Policy*, 6(2), 143-166.

McGettrick, A. (2013). Toward effective cyber security education. *IEEE Security & Privacy*, 11(6), 66-68.

Mitchell, L. (2020). Cybersecurity in education: Protecting student and staff data. *Journal of Educational Technology*, 37(2), 65-78. https://doi.org/10.1016/j.jeduc.2020.07.005

National Institute of Standards and Technology (NIST). (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2018). *NIST Cybersecurity Framework Version 1.1*. Retrieved from https://www.nist.gov/cyberframework.

Olavsrud, T. (2020). Protecting research data in universities: Challenges and best practices. *CIO*. Retrieved from https://www.cio.com/article/3523745/protecting-research-data-in-universities-challenges- and-best-practices.html

Ponemon Institute. (2021). *Cost of a data breach report 2021*. Retrieved from https://www.ibm.com/security/data-breach

Rahman, N. A. A, Sairi I. H., Zizi N. A. M., & Khalid F. (2020). The importance of cybersecurity

education in school. International Journal of Information and Education Technology, 10(5),

San Diego Unified School District. (2018). Data breach information. Retrieved from https://www.sandiegounified.org

Shafiq, M., & Gu, Q. (2019). Cybersecurity in education: Emerging challenges and solutions. *IEEE Access*, 7, 94472-94484. https://doi.org/10.1109/ACCESS.2019.2927715

Shin, D. (2018). Cybersecurity in K-12 education: A guide to understanding and preventing ransomware attacks. *Educational Technology & Society*, 21(4), 125-136.

Smith, A. B., & Jones, C. D. (2021). Best practices for cyber security in educational institutions. *International Journal of Educational Technology in Higher Education*, 18(1), 1-18.

United States Department of Education. (2020). Cybersecurity Resource Center. Retrieved from https://www.ed.gov/cybersecurity.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20.

Yamba L. I, & Abwino, W. P. (2023). Teachers as catalysts for digital transformation and cyber security in schools: Lessons from Northern Region in Zambia. *International Journal of Multidisciplinary Research and Development 10*(10), 72-77.