SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 2 | February 2025 - Peer Reviewed Journal

CYBERSECURITY CHALLENGES, STRATEGIES AND EMERGING TRENDS IN HIGHER EDUCATION INSTITUTIONS – A SURVEY

Suzzanne Nzingo Kalume[1], Dr. Shadrack Ochieng Owiti[2]
[1,2]Jaramogi Oginga Odinga University of Science & Technology (JOOUST)

Article DOI: https://doi.org/10.36713/epra19824
DOI No: 10.36713/epra19824

ABSTRACT

Since the COVID-19 pandemic, significant progress has been made toward digitalization, with nearly every aspect of life now heavily reliant on technology. In this digital age, higher education institutions have been compelled to transition most, if not all, of their operations online, hence expanding the cyber landscape. Several studies show the education sector has become a prime target for cyberattacks, with Higher Education Institutions (HEIs) accounting for 86% of such attacks. These incidents continue to rise weekly, driven by the vast amounts of sensitive data HEIs manage, the diverse user base operating within and beyond their networks and the open nature of their systems and networks. Cyber threats and attacks have severe consequences for any organization, including HEIs, causing reputational damage, financial losses, legal disputes and operational disruptions. It is imperative for HEIs to implement robust strategies and best practices to mitigate and reduce the risk of cyberattacks. This paper presents a survey of research published between 2020 and 2024, looking into the strategies, emerging trends and challenges in HEI cybersecurity. Additionally, it proposes the need for future studies to explore how emerging technologies such as Artificial Intelligence (AI), Blockchain and the Internet of Things (IoT) can enhance cybersecurity. As technology continues to evolve rapidly and societies continue to depend on information systems, these emerging technologies advancements have significant potential for strengthening cybersecurity measures.

KEYWORDS: *Cybersecurity, Higher Education Institutions, HEIs, Challenges, Strategies, Emerging trends*

INTRODUCTION

In the digital age, the prevalence of cyber threats has been rising at an alarming rate. Scholz et al., 2021 states that Cyber-attacks have been on the rise not just in frequency but also in sophistication and ransom demand. A report by the Communications Authority of Kenya indicates a 16.5% increase in cyber threats between April 2023 and April 2024 signifies how Cybercriminals have become sophisticated in their methods. Unaddressed cyber-attacks can result in disruption of operations, financial losses, legal disputes and reputational damage; hence organizations should implement robust defense mechanisms and adopt proactive measures to safeguard against cyberattacks.

No organization is entirely secure, as cybercriminals increasingly employ sophisticated technologies to achieve their objectives; HEIs are not immune. According to Verizon's 2020 report, the primary motivation for cybercriminals is financial gain, which accounts for 86% of incidents, followed by espionage at 10% (Stealthlabs, 2021). The academia sector has been ranked 4th and 2nd as the most targeted by Communications Authority (CA) of Kenya (September 2024), and Microsoft's Cyber Signals (2024) reports respectively signifying that the academia sector is an attractive target for cyber attackers Universities and tertiary colleges, which constitute the academia sector, are vulnerable due to several factors, including the vast amount of sensitive data they handle, legacy infrastructure, open network systems and a diverse user base. In 2022, a U.S.-based research firm reported that the cyberattack landscape for higher education institutions (HEIs) is growing at an alarming rate, with a weekly growth of 75%. The education sector, in comparison to other industries, has been affected immensely by cyber-attacks, which have doubled since the COVID-19 pandemic. (Scholz et al., 2021).

The digital landscape of HEIs, encompasses personal devices, online course materials, web applications, research data, student records, cloud-based applications and virtual learning environments. Cybercriminals exploit the vulnerabilities to infiltrate university networks, posing serious risks to institutional operations and data security.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 2 | February 2025 - Peer Reviewed Journal

PROBLEM STATEMENT

In the digital age, higher education institutions (HEIs) increasingly rely on technology to fulfil their core mandates, achieve strategic goals and meet the needs of tech-savvy stakeholders in a rapidly evolving digital landscape. While this digital transformation offers numerous opportunities, it also exposes HEIs to significant cybersecurity risks, making them attractive targets for cybercriminals. Studies reveal that HEIs face unique challenges in safeguarding their digital ecosystems, including budget constraints, outdated infrastructure, open networks, and a lack of training and awareness. The repercussions of cyberattacks can be severe, including financial losses, reputational damage, negative publicity, and disruptions to institutional credibility. It is therefore critical for HEIs to implement sound cybersecurity strategies to mitigate these risks. However, limited research exists that holistically addresses the intersection of cybersecurity challenges, strategies, and emerging trends in higher education. Most existing studies focus on isolated aspects, such as frameworks for institutional adoption.

This paper aims to bridge this gap by exploring the cybersecurity challenges, strategies and emerging trends specific to higher education institutions. It seeks to answer the central research question: What are the cybersecurity challenges, strategies and emerging trends in higher education institutions?

OBJECTIVES

This paper aims to bridge this gap by exploring the cybersecurity challenges, strategies and emerging trends specific to higher education institutions.

RESEARCH QUESTIONS

What are the cybersecurity challenges, strategies and emerging trends in higher education institutions?

SCOPE OF STUDY

This study focuses on higher education institutions, specifically universities and colleges worldwide. It examines their unique cybersecurity challenges, strategies and emerging trends, considering variations in technological adoption, institutional policies and resource availability.

LITERATURE REVIEW

Theoretical Framework

The table below presents the relevant theories to the study

Table 1: The relevant theories applicable to the study

Theory	Concept	Relevance	Application
Socio-technical Systems (STS) Theory	Emphasizes on 2 key factors human and technical aspects that go together in the race against cyber threats and attackers (Mahmood et al., 2024)	Enhancing cybersecurity within organizations requires both social aspects (e.g., human factors i.e. skills and attitudes, organizational dynamics) and technical aspects (e.g., technology, tasks and processes) to work together effectively (Mahmood et al., 2024; Zoto et al., 2019).	Organizations can train and upskill staff, raise awareness for staff, and also implement cybersecurity processes, procedures and technologies.
Technology Organization Environment (TOE)	Posits that adoption and implementation of technology is dependent on the technological, Organizational and environmental factors (Hasani et al., 2023)	The implementation of cybersecurity technologies depends on and affects three key contexts: technology, organization, and environment (Hasani et al., 2023)	Organizations can implement robust cybersecurity technologies to detect and defend against threats, as part of the technological context. Additionally, staff training and awareness can be addressed within the organizational context, while compliance with regulatory standards can be ensured through the environmental context
Game theory	In every game, players must understand the behaviour of their opponents to make strategically rational decisions (Patil, 2018).	Drawing from game theory, organizations can enhance cybersecurity by understanding the behavior of attackers and proactively developing defense mechanisms (Patil, 2018).	That organizations can establish predictive defense mechanisms to effectively defend, protect and respond accordingly to cyber threats and attacks

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 2 | February 2025 - Peer Reviewed Journal

SIGNIFICANCE OF CYBERSECURITY

Cybersecurity measures and strict adherence to best practices are critical for organizations in the rapidly evolving digital landscape to ensure prevention, protection, continuity and resiliency. Cybersecurity entails the practices, technologies and policies put in place to prevent cyberattacks or mitigate the impact of attacks and threats (Lindemulder & Kosinski, 2024). For institutions to remain operational and achieve their strategic objectives, cybersecurity must be prioritized and treated with the seriousness it demands. A robust cybersecurity framework not only prevents potential breaches but also ensures that, in the event of an incident, institutions can swiftly recover and maintain business continuity (Safitra et al., 2023; Thomas & Sule, 2022). This capability to resume operations is crucial for minimizing disruptions and sustaining trust among stakeholders.

Table 2: Cybersecurity Statistics

Statistics	*Description*
2507	Average number of Weekly cyberattack attempts on Education institutions (Microsoft Threat Intelligence, 2024)
43%	of HEIs attacked weekly in UK (Microsoft Threat Intelligence, 2024)
88%	of Cybersecurity breaches caused by human error Stanford Research, (CISOMAG, 2020)
USD 4.88 Million	Average cost of a data breach 2024 (IBM Report, n.d.)
77%	of organizations do not have an Incident Response Plan in place (Sobers, 2024)
43%	Data loss is the most expensive element of a cyberattack accounting for 43% of the total cost (IBM Report, n.d.)

Cybersecurity plays a significant role in ensuring the confidentiality, integrity and availability of the vast repositories of sensitive information, which includes personal identification data, financial records, intellectual property and research outputs (Nassoura, 2022). Protection of digital assets is crucial to ensure institutional integrity, prevent unauthorized access, theft or misuse, prevent disruption of academic and administrative operations and maintain compliance with regulatory and ethical standards. Achieving this goal is particularly challenging in HEIs context, where an open and collaborative environment is essential to fostering academic freedom and innovation. Cybersecurity measures must strike a delicate balance, enabling secure operations while preserving the accessibility needed for research and learning (Gupta et al., 2021). Effective cybersecurity measures protect organizations from a range of adverse outcomes, such as financial losses, legal liabilities, regulatory fines and reputational damage (Smith & Jones, 2020). These consequences can have a long-term impact on an institution's credibility and operational capacity. By adopting comprehensive cybersecurity strategies, HEIs can build resilience against cyber threats while maintaining their mission of openness and accessibility.

Cybersecurity in Higher Education Institutions

Since the COVID-19 pandemic, HEIs have not just become a profitable target but also an attractive target for cyberattacks due to the open nature of their networks and the sensitivity of the vast data they store and process (Hobbs, 2023). The open network architecture of HEIs is designed to accommodate a diverse range of users which includes students, faculty, staff, vendors, suppliers and external collaborators. The openness fosters academic collaboration and accessibility, but also introduces significant vulnerabilities (Cheng & Wang, 2022). In the digital age, with classes, meetings, remote work being conducted online, the attack surface or potential vector for cyberattack have expanded in recent years. The sensitivity and diversity of data managed by HEIs, including personal identification information (PII), academic records, financial information, research data, medical records and intellectual property, make these institutions lucrative targets for cybercriminals (Cheng & Wang, 2022). A successful breach of this data can result in severe consequences, including reputational damage, legal implications, operational disruption, loss of trust among prospective students, staff and partners as well as financial losses. Consequently, it is imperative that HEIs prioritize cybersecurity strategies to mitigate against potential risks associated with such attacks (Yusif & Hafeez-Baig, 2023). HEIs need to invest in modern infrastructure, capacity building, implement strict access controls and allocate adequate budgets to sustain robust cybersecurity initiatives (Stefan, 2024).

Table 3: Common Cyberattacks to HEIs

Social engineering	A cyberattack where a victim is tricked into giving out valuable information or compelled to download a malware or click links which exposes them to cybercrime
Ransomware attacks	An attack that encrypts crucial data, making systems and data inaccessible until a ransom is paid
Distributed Denial of Service (DDoS) Attack	An attack that floods or overwhelms the network with traffic leading to inaccessibility or unavailability of online services or resources or cause system downtime
Insider threat	An attack as a result of intentional or unintentional compromise of security by a student or a staff who has authorised access
Malware attacks	An attack that infiltrates systems causing malfunction, compromise data integrity and operational disruption
Data breaches	An attack where unauthorized individuals get access to sensitive data such as student academic records, financial data, medical records, etc.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 2 | February 2025 - Peer Reviewed Journal

RESEARCH DESIGN

Methodology

The methodology entailed conducting systematic searches in academic databases namely Google Scholar, Directory Open Access Journal (DOAJ), Web of Science (WoS) and IEEE Xplore. The key search terms was based on recency (publications between 2020 to 2024) and relevance (keywords: cybersecurity, higher education institutions, HEIs, University, strategies, challenges and emerging trends). The inclusion criteria considered papers that have been peer-reviewed, published within the last five years and are accessible. Papers that did not meet these criteria were excluded.

RESEARCH FINDINGS

Challenges to Cybersecurity in Higher Education Institutions

Organizations, including higher education institutions (HEIs), face a myriad of cybersecurity challenges as they navigate an increasingly digital and interconnected world. One major challenge is the rise in sophisticated cyberattacks, such as ransomware and phishing, which target critical infrastructure and sensitive data (CISA, 2023). The diversity of users in higher education institutions which includes faculty, students and external partners, creates complex networks prone to vulnerabilities (Grama, 2020). The variety of data in HEIs is also a challenge to cybersecurity as it includes personal identification information (PII), academic records, financial information, research data, medical records and intellectual property (Fouad, 2021). The limited financial resources and budgetary constraints further hinder the ability of institutions to implement advanced security measures (EDUCAUSE, 2022; Cheng & Wang, 2022). Additionally, balancing the need for open access to information with stringent security protocols poses significant difficulties (Chen et al., 2021). The "Bring Your Own Device" (BYOD) policy presents a significant challenge to cybersecurity in HEIs as users use their unsecured personal devices to access institutional networks, thus create vulnerabilities within the network (Cheng & Wang, 2022; Fouad, 2021). Another challenge is inadequate cybersecurity training and awareness of users and shortage of skilled IT and cybersecurity professionals within the University community network results in inadequate preparedness to prevent, detect or respond effectively to cyber incidents (Blažič, 2021; Otoom et al., 2024; Ramos & Ii, 2022; Triplett, 2023). Outdated infrastructure is another pressing issue where legacy systems and technologies are not regularly updated or patched creating exploitable vulnerabilities (Ulven & Wangen, 2021).

Cybersecurity Strategies for HEIs

Cybersecurity entails the practices, technologies and policies put in place to prevent cyberattacks or mitigate the impact of attacks and threats (Lindemulder & Kosinski, 2024). Cybersecurity is essential for creating a secure digital environment for all organizations, including HEIs. The HEIs are highly targeted due to the nature of the sensitive and diverse data they have, hence the need to implement robust mechanisms and strategic measures to prepare for potential threats, prevent breaches and swift response to mitigate the impact. (Alexei, 2021). Effective cybersecurity strategies ensure the continuity of operations and safeguard the HEIs ecosystem facilitating achievement of their goals and objectives.

HEIs must align their cybersecurity frameworks with broader regulatory and ethical considerations to strike a balance between accessibility and security. This involves implementing policies and procedures that promote secure access and use without stifling academic collaboration (Fouad, 2021). By developing an institutional cybersecurity culture and operations, HEIs can create a secure digital environment that supports the academic and research missions without compromising on safety (Cheng & Wang, 2022; Uchendu et al., 2021). Governance as a strategy entails top management support in developing and strengthening a robust institutional cybersecurity culture (Liu et al., 2020). The establishment and enforcement of Cybersecurity policies and procedures guide users on the proper use of digital asset, including responding to potential risks and threats. (Cheng & Wang, 2022; Yusif & Hafeez-Baig, 2023). Establishing a defence mechanism is key in enhancing monitoring of potential threats for early response and effective mitigation (Liluashvili, 2021). Robust capacity-building for staff and students on cybersecurity best practices is critical to foster a strong cybersecurity culture, this significantly mitigates human error which remains to be the weakest link in any organization (Hobbs, 2023). HEIs should comply with the recommended standards, like COBIT, ITIL, ISO 27000 series for ISMS (information security management system), Data protection Act, to ensure a secure digital ecosystem (Nuñez et al., 2023). HEIs should implement a comprehensive incident response plan to facilitate proactive and swift response to cyber threats thus ensuring institutional resilience, effective recovery, operational continuity and trust of students, staff and faculty (Alexei, 2021; Miller, 2024). Another strategy is by incorporating emerging technologies such as AI, machine learning (ML) and blockchain for enhancing intrusion detection, anomaly detection and identification of human risk factors to address vulnerabilities.

Emerging Trends

Emerging trends in cybersecurity are reshaping how organizations, including higher education institutions, address digital threats. Recent advances in AI technologies in this digital age has come with its fair share of benefits and challenges to individuals, organizations and businesses at large. One notable trend is the increased use of artificial intelligence (AI) and machine learning (ML) to detect and respond

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 2 | February 2025 - Peer Reviewed Journal

to cyber threats in real-time, enhancing predictive capabilities (Sharma & Kumar, 2022). But also, on the other hand, the cyberattack landscape is increasingly expanding with AI-based attacks (Kaloudi & Li, 2020; Cheng & Wang, 2022) which are likely to impact the cybersecurity position of organizations in the digital age. The adoption of Internet of Things (IoT) technologies significantly increases the vulnerability of an organization's digital ecosystem to cyberattacks and criminal activities (Cheng & Wang, 2022). IoT devices which are connected to the organizations network are characterized by limited built-in security features, hence, present an expanded attack surface for cybercriminals. These vulnerabilities can be exploited to gain unauthorized access, disrupt operations and steal sensitive data. As organizations integrate and adopt AI and IoT technologies to enhance operational efficiency and innovation, it becomes vital to implement robust cybersecurity measures to mitigate associated risks.

CONCLUSION & RECOMMENDATIONS

Going forward, HEIs should build resilience through collaboration, awareness and leveraging on new and emerging technologies. In conclusion, addressing cybersecurity in higher education institutions requires a comprehensive approach that balances robust strategies, an understanding of prevailing challenges, and adaptation to emerging trends. Institutions must prioritize implementing multi-layered defenses, regular training and proactive incident response plans to mitigate vulnerabilities. Challenges such as limited resources, regulatory compliance and the complexity of diverse user networks highlight the need for innovative and cost-effective solutions. Leveraging emerging trends like AI-driven threat detection, Zero Trust Architecture and user-centric security measures can enhance resilience against evolving cyber threats. Moving forward, collaboration between institutions, policymakers, and technology providers will be critical to fostering shared knowledge and resources. Future research could explore scalable cybersecurity solutions tailored to the unique operational and educational needs of higher education, ensuring that institutions remain secure while maintaining their commitment to open access and academic freedom as well as methods to detect and mitigate AI-enabled threats and IoT vulnerabilities in higher education institutions.

REFERENCES

1. *Alexei, A. (2021). CYBER SECURITY STRATEGIES FOR HIGHER EDUCATION INSTITUTIONS. Journal of Engineering Science. https://doi.org/10.52326/jes.utm.2021.28(4).07*
2. *Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. Technology in Society, 67, 101769. https://doi.org/10.1016/j.techsoc.2021.101769*
3. *Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Inf., 13. https://doi.org/10.3390/info13040192*
4. *CISOMAG. (2020, September 12). "Psychology of Human Error" Could Help Businesses Prevent Security Breaches. CISO MAG | Cyber Security Magazine. https://cisomag.com/psychology-of-human-error-could-help-businesses-prevent-security-breaches/*
5. *Fouad, N. S. (2021). Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526*
6. *Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business & Economics, 3(5), 97. https://doi.org/10.1007/s43546-023-00477-6*
7. *Hobbs, J. (2023). Cybersecurity awareness in higher education: A comparative analysis of faculty and staff. 24(1), 159–169. https://doi.org/10.48009/1_iis_2023_114*
8. *IBM Report. (n.d.). Cost of a data breach 2024 | IBM. Retrieved November 29, 2024, from https://www.ibm.com/reports/data-breach*
9. *Kaloudi, N., & Li, J. (2020). The AI-Based Cyber Threat Landscape: A Survey. ACM Comput. Surv., 53(1), 20:1-20:34. https://doi.org/10.1145/3372823*
10. *Liluashvili, G. B. (2021). Cyber Risk Mitigation in Higher Education. Law and World. https://doi.org/10.36475/7.2.2*
11. *Lindemulder, G., & Kosinski, M. (2024, August 12). What Is Cybersecurity? | IBM. https://www.ibm.com/topics/cybersecurity*
12. *Liu, C.-W., Huang, P., & Lucas Jr., H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. Journal of Management Information Systems, 37(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190*
13. *Mahmood, S., Chadhar, M., & Firmin, S. (2024). Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective. Applied Sciences, 14(24), Article 24. https://doi.org/10.3390/app142411610*
14. *Microsoft Threat Intelligence, M. T. (2024, October 10). Cyber Signals: Cyberthreats in K-12 and higher education. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2024/10/10/cyber-signals-issue-8-education-under-siege-how-cybercriminals-target-our-schools/*
15. *Miller, J. (2024, August 27). The Importance of Incident Response in Higher Education. Bitlyft. https://www.bitlyft.com/resources/the-importance-of-incident-response-in-higher-education*
16. *Nassoura, A. B. (2022). Cybersecurity Technologies And Practices In Higher Education Institutions: A Systematic Review. 19(3).*
17. *Nuñez, M., Palmer, X.-L., Potter, L., Aliac, C. J., & Velasco, L. C. (2023). ICT Security Tools and Techniques among Higher Education Institutions: A Critical Review. International Journal of Emerging Technologies in Learning (iJET), 18(15), 4–22. https://doi.org/10.3991/ijet.v18i15.40673*

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 2 | February 2025 - Peer Reviewed Journal

18. *Otoom, A. A., Atoum, I., Al-Harahsheh, H., Aljawarneh, M., Refai, M. N. A., & Baklizi, M. (2024). A collaborative cybersecurity framework for higher education. Information & Computer Security, ahead-of-print(ahead-of-print). https://doi.org/10.1108/ICS-02-2024-0048*
19. *Patil, A. P. (2018). Applications of Game Theory for Cyber Security System: A Survey. 13(17).*
20. *Ramos, N. M. D., & Ii, F. D. E. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. International Journal of Evaluation and Research in Education (IJERE). https://doi.org/10.11591/ijere.v11i3.22863*
21. *Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability, 15(18), Article 18. https://doi.org/10.3390/su151813369*
22. *Scholz, S., Hagen, W., & Lee, C. (2021). The Increasing Threat of Ransomware in Higher Education. EDUCAUSE Review. https://er.educause.edu/articles/2021/6/the-increasing-threat-of-ransomware-in-higher-education*
23. *Sobers, R. (2024, September 13). 157 Cybersecurity Statistics and Trends [updated 2024]. https://www.varonis.com/blog/cybersecurity-statistics*
24. *Stealthlabs. (2021). Cybersecurity Threats and Attacks: All You Need to Know. Stealthlabs. https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/*
25. *Stefan. (2024, November 1). The Future of Cybersecurity: Why Proactive Strategies are Key to Protecting Your Business. Stefanini. https://stefanini.com/en/insights/news/fundamentals-of-cybersecurity-how-it-can-protect-your-business*
26. *Thomas, G., & Sule, M.-J. (2022). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. Organizational Cybersecurity Journal: Practice, Process and People, 3(1), 18–40. https://doi.org/10.1108/OCJ-09-2021-0025*
27. *Triplett, W. J. (2023). Addressing Cybersecurity Challenges in Education. International Journal of STEM Education for Sustainability. https://doi.org/10.53889/ijses.v3i1.132*
28. *Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387*
29. *Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 13(2), Article 2. https://doi.org/10.3390/fi13020039*
30. *Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework. Journal of Applied Security Research, 18(2), 267–288. https://doi.org/10.1080/19361610.2021.1989271*
31. *Zoto, E., Kianpour, M., Kowalski, S. J., & Lopez-Rojas, E. A. (2019). A Socio-technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education. Complex Systems Informatics and Modeling Quarterly, 18, 65–75. https://doi.org/10.7250/csimq.2019-18.04*
32. *Gupta, R., Sharma, S., & Patel, A. (2021). Cybersecurity challenges in educational institutions: Trends and solutions. Journal of Information Security, 12(4), 134-145. https://doi.org/10.1016/j.jisec.2021.12.004*
33. *Smith, J., & Jones, P. (2020). Safeguarding academic data: Strategies for cybersecurity in higher education. Cybersecurity Review, 8(3), 112-123. https://doi.org/10.1016/j.cyrev.2020.08.012*

Acknowledgement
I am deeply grateful to God for His provision and for granting me this opportunity. I sincerely appreciate my family for their unwavering support and encouragement. I also extend my heartfelt gratitude to my lecturer for his valuable guidance throughout this process.

Author & Co-author

1. Suzzanne Nzingo Kalume	**PhD Student** Jaramogi Oginga Odinga of Science & Technology (JOOUST)
2. Dr. Shadrack Ochieng Owiti	**Lecturer** Jaramogi Oginga Odinga of Science & Technology (JOOUST)