**Expert Journal of Business and Management,** Volume 12, Issue 2, pp.67-73, 2024
 ISSN 2344-6781
http://Business.ExpertJournals.com

# A Narrative Review on Enhancing Cybersecurity in Higher Education Institutions: The Role of Continuous Training and Awareness

Constance MOUWERS-SINGH* and Tichaona Buzy MUSIKAVANHU

Boston City Campus, South Africa

*This narrative review article problematises cybersecurity in the higher education sector. It highlights the importance of fostering a continuous training and awareness culture to reduce cyber incidents and threats. Post-COVID-19, universities face increased cyberattack frequency globally, necessitating urgent and effective responses. This study provides an understanding of the role of continuous training and awareness in effectively combating and mitigating cyber threats in higher education institutions (HEIs). This article highlights the pivotal role of user education in cybersecurity. Establishing formal processes to educate students and staff about digital risks and safe information technology practices is crucial. This education extends beyond awareness; it encompasses actionable strategies to secure institutional cyberspace. The findings reveal that although technology can help fight cybercrime, the most effective way to combat these threats lies in comprehensive training and awareness-raising among students and staff within HEIs. The review concludes that continuous training and awareness equip individuals to handle cyber threats better and significantly lower institutional risks. This article contributes to the discourse by offering insights into how HEIs can develop resilient cybersecurity frameworks through focused training and awareness programs, ultimately fostering a safer digital environment in an increasingly interconnected world.*

***Keywords:*** *higher education institutions, cybersecurity, cybercrime, COVID-19*

***JEL Classification****: M10; I23*

## 1. Introduction

The rapid digital transformation necessitated by the COVID-19 pandemic has significantly altered how higher education institutions (HEIs) operate globally. While enabling continued educational activities, this shift has also increased cybersecurity risks (Haque et al., 2023; Hijji and Alam, 2022; Xiao et al., 2023). In addition to creating new vulnerabilities, the pandemic's drive for remote work and online learning platforms has accelerated the sophistication of cyber threats. As a result, HEIs are grappling with increased cyberattacks,

*Corresponding Author:
Constance Mouwers-Singh, Boston City Campus, South Africa

Article History:
Received 7 February 2024 | Accepted 8 August 2024 | Available online 30 September 2024

Cite Reference:
Mouwers-Singh, C. and Musikavanhu, T.B., 2024. A Narrative Review on Enhancing Cybersecurity in Higher Education Institutions: The Role of Continuous Training and Awareness. *Expert Journal of Business and Management, 12(2),* pp.67-73.

leading to substantial financial and intellectual property losses (Alexei, 2021; Dioubate and Wan Daud, 2022; Hijji and Alam, 2022).

In South Africa, the proliferation of the Internet of Things (IoT) market is projected to reach $31.6 billion by 2028 (Mushwana, 2023), which exemplifies the rapid digital adoption, further elevating the risk of cybercrime. This is echoed globally, with HEIs facing escalating threats and the consequent necessity for robust cybersecurity measures. However, despite the increasing prevalence of security technologies, HEIs continue to experience breaches, underscoring the inadequacy of current strategies (Badamasi and Utulu, 2021; Dioubate et al., 2023; Maranga and Nelson, 2019).

The internet has revolutionised how people communicate, conduct business and study. Various organisations, including HEIs, now store some of their data and conduct teaching and learning activities online, a transition that offers both convenience and increased risk of cybercrime (Al-Alawi et al., 2020; Haque et al., 2023; Xiao et al., 2023). According to a 2021 report by Interpol, the rapid pace of digital transformation fosters new types of cyberattacks and creates more opportunities for cybercriminals (Interpol, 2021). This report also reveals that in 2021, South Africa experienced over 230 million cyber threats, with 219 million email threats. The country has also become a primary target for ransomware attacks in Africa (Interpol, 2021). Despite these growing threats, the issue of cybercrime within educational institutions remains relatively under-researched. This article addresses this gap by proposing specific measures to help HEIs minimise their vulnerability to cybercrimes (Al-Alawi et al., 2020; Dioubate et al., 2023).

HEIs invest substantial financial resources in sophisticated software and hardware systems, including intrusion detection systems, antivirus and antispyware software, and encryption mechanisms (Dioubate and Wan Daud, 2022; Hijji and Alam, 2019). These technological solutions alone are, however, insufficient against the continuously evolving cyber threats. There is an increasing need for cybersecurity awareness and training, particularly for remote workers who are more exposed to these risks (Hijji and Alam, 2022). While HEIs are upgrading their security tools and strategies to combat the latest cyber threats, cybercriminals are concurrently developing new methods to circumvent these defences (Dioubate et al., 2023; Haque et al., 2023; Maranga and Nelson, 2019). This review study, therefore, seeks to provide an understanding of how HEIs can better prepare and create defence systems against cyberattacks by adopting a culture of continuous training and awareness to mitigate cybercrime risks.

## 2. Methods

This narrative review article employs a structured and comprehensive literature review methodology to collect, analyse, and synthesise existing research, elucidating cybersecurity in HEIs. Following Snyder's (2019) assertion of the literature review's significance in contemporary research for compiling and synthesising prior studies, this review aims to build upon existing knowledge and promote discourse on the topic within the HEIs context.

The literature review is a scholarly examination of various sources pertinent to the research area. This process involves gathering information and providing critical descriptions, summaries, and evaluations of each source (Ramdhani et al., 2014). The sources selected for this review were diverse to ensure a comprehensive understanding of the topic. Key articles from academic journals were primarily sourced through Google Scholar, supplemented by reports, conference and symposium papers, relevant online sources, and books.

The selection process was guided by specific search keywords: "cybercrime," "cybersecurity," "continuous learning and training," and "cybercrime awareness." Additionally, the keywords "cybercrime and higher education" were utilised to broaden the search scope, focusing on the intersection of cybercrime and higher education. These keywords were applied strategically in the journal papers' titles, keywords section, and text discussions to identify the most relevant literature. Each source was meticulously evaluated to ensure it aligned with the study's objectives and contributed meaningfully to the debate. The researcher organised the literature logically, selecting materials that best fit the study's parameters and ensuring a well-rounded topic exploration.

The breakdown of the sources is as follows:

***Table 1**. Information source types and numbers*

| Information Source Type | Number of Sources used |
|---|---|
| Journal papers | 21 |
| Pertinent Internet sources | 4 |
| Books | 2 |
| Conference and Symposium Papers | 3 |
| Reports | 1 |
| Total number of Sources used | 31 |

In total, 31 sources were used to inform this review, spanning publications from 2006 to 2023. This time frame was selected to capture a comprehensive view of cybersecurity's evolution and current state in HEIs, reflecting historical context and contemporary developments.

Through this meticulous and diverse literature review, the article aims to present a nuanced and in-depth understanding of cybersecurity challenges in HEIs, highlighting the importance of continuous training as well as the role of awareness in mitigating these risks. The methodology underpins the review's goal of providing a holistic perspective, drawing on various scholarly and practical insights.

## 3. Discussion

### 3.1. Building a Cybersecurity Culture in HEIs

The narrative review underscores the necessity of developing a cybersecurity culture within HEIs through ongoing training and awareness initiatives. Cheng and Wang (2022) and Al-Alawi, Al-Kandari, and Abdel-Razek (2016) highlight the importance of continuous education and awareness campaigns in keeping the workforce informed about cybersecurity. This approach is essential in light of the numerous unintentional cybersecurity threats observed since the introduction of regulations like the POPI Act (van Niekerk, 2017). The prevalence of cyber threats such as phishing, as noted by Alexei (2021) and Maranga and Nelson (2019), further emphasises the need for such ongoing training programs. The human factor remains a significant vulnerability, necessitating a shift from solely technology-based solutions to a more holistic approach incorporating human-centred strategies (Colwill, 2009).

### 3.2. Cybercrime in Higher Education Institutions

The digital transformation in universities has increased the vulnerability of HEIs to cybercrime. Anderson, Abiodun, and Christoffels (2020) highlight IT teams' challenges in securing diverse and multiplying digital devices. The increased exposure to cyber threats like malware and phishing attacks is exacerbated by a general lack of cybersecurity knowledge among students and staff (Cojocariu et al., 2020; Alexei, 2021). Implementing laws like the POPI Act highlights the need for legal compliance and proactive training to mitigate these risks (Charandura, 2022). However, the effectiveness of such measures is often limited by the lack of integration of cybersecurity awareness into the strategic objectives of most academic institutions (Alharbi and Tassaddiq, 2021).

### 3.3. A Continuous Learning Culture

The review reveals that establishing a continuous learning culture within HEIs is pivotal in combating cyber threats. Ongoing professional training and fostering a culture of cyber resilience are critical in this regard (Chanani and Wibowo, 2019; Ciuchi, 2022). This culture should address the evolving nature of cyber threats and focus on building resilience through regular internal audits, penetration tests, and phishing simulations (AIICT Team, 2022; Le et al., 2019). Moreover, the need for ongoing cybersecurity education and awareness training is vital, given the continuously evolving nature of cyber threats (Cheng and Wang, 2022).

### 3.4. Cybercrime Education, Cybersecurity Training and Awareness

The review also highlights the critical role of cybercrime education and learning in HEIs. Most cyberattacks exploit human factors through social engineering, making user education imperative (Alexei, 2021). Cheng and Wang (2022) advocate for building a cybersecurity culture to promote good security behaviours. This involves training and ensuring that all stakeholders understand their roles and responsibilities in maintaining cybersecurity (Anderson et al., 2020). The importance of ongoing security training and awareness, especially in light of high staff turnover, cannot be overstated (Colwill, 2009). Training programs must be human-centric to ensure effective content uptake and adaptability to the constantly evolving digital landscape (Cheng and Wang, 2022; Muniandy et al., 2017).

## 4. Conclusion

The narrative review presented in this paper provides a comprehensive analysis of the cybersecurity challenges facing HEIs in the wake of rapid digital transformation and the increasing sophistication of cyber threats. The key findings from the literature underscore the critical need for HEIs to develop a robust cybersecurity culture, emphasising the role of continuous training, awareness, and organisational learning culture in mitigating these risks.

The review highlights that while technological advancements in cybersecurity are essential, they are insufficient. The human factor, as pointed out by Alexei (2021), Cojocariu, Verzea, and Chaib (2020), and Colwill (2009), plays a crucial role in the cybersecurity ecosystem of HEIs. Continuous education and awareness programs are necessary to keep staff and students abreast of the latest cybersecurity threats and best practices (Cheng and Wang, 2022: Alharbi and Tassaddiq, 2021).

Furthermore, integrating cybersecurity into the strategic objectives of HEIs is not just a technological issue but also a social one, as Anderson et al. (2020) argued. The evolving nature of cyber threats requires a dynamic approach to cybersecurity education that adapts to the changing landscape and prepares the institution's community for emerging risks. This approach should include regular training exercises like penetration tests and phishing simulations to build a proactive and resilient cybersecurity posture (AIICT Team, 2022; Le et al., 2019).

Additionally, the review indicates the importance of compliance with data protection laws, such as the POPI Act, and underscores the need for HEIs to not only adhere to these laws but to go beyond compliance in fostering a secure digital environment (Charandura, 2022; van Niekerk, 2017). Effective cybersecurity management in HEIs involves a comprehensive strategy that combines legal compliance, technological solutions, and, most importantly, a human-centric approach to security awareness and education.

This narrative review demonstrates that the path to enhancing cybersecurity in HEIs lies in cultivating a continuous learning culture, where ongoing training and awareness are integral components. This approach will equip individuals within these institutions to handle emerging cyber threats effectively and contribute to a broader cultural shift towards improved cybersecurity practices. The insights from this review are critical for HEIs as they navigate the complexities of the digital age, striving to protect their networks, data, and communities from the ever-evolving landscape of cyber threats.

## 5. Recommendations

This section consolidates and enhances the recommendations and suggestions highlighted throughout the review. It extends the conclusions drawn and provides actionable strategies for HEIs to bolster their cybersecurity posture.

- Fostering communities of practice: As Cheng and Wang (2022) suggest, establishing communities of practice can deepen understanding and contextualise cybersecurity practices, creating an environment where knowledge and experiences are shared effectively.
- Accessible online repository for cybersecurity training: Maintaining a comprehensive online repository of all cybersecurity training materials allows for continuous access and revisiting of vital information, ensuring ongoing learning.

- Enhanced security awareness methods: Abawajy (2014) highlights the necessity of examining and improving security awareness delivery methods from the recipient's perspective. This can lead to more effective and engaging awareness programs.
    a) Routine skill assessment tests: Regularly assessing employees' cybersecurity skill levels can help identify areas needing improvement (Zur, 2022).
    b) Feedback-driven cybersecurity training: Regular surveys to gauge the effectiveness of cybersecurity training and hard-to-spot cybercrime tests can enhance the quality and relevance of training programs.
- Incorporating cybersecurity education in curricula: Integrating cybersecurity education into student syllabi prepares and equips them against cybercrime and threats (Muniandy et al., 2017).
- A multi-faceted approach to skill development: Adopting a multi-faceted approach involving education, collaboration, research, and awareness is crucial for protecting critical infrastructure (Mushwana, 2023).
- Consistent and diverse user awareness training: HEIs should implement regular user awareness training, addressing various issues from email and password hygiene to internet usage best practices (Anderson et al., 2020).
- Public-private collaboration: Encouraging collaboration between public and private sectors can facilitate knowledge sharing and the adoption of best practices (Mushwana, 2023).
- Varied training delivery methods: Diverse delivery methods for training programs, such as video, text, or game-based approaches, can cater to adult learning preferences and enhance engagement (Alharbi and Tassaddiq, 2021).
- Targeted training for IT professionals: Focusing cybersecurity awareness training on IT professionals can foster a more robust security culture within institutions (van Niekerk, 2017).
- Comprehensive phishing exercise training: Structured and extensive phishing training programs can significantly reduce the likelihood of email-based cybercrimes (Miranda, 2018).
- Utilising social media for learning: Platforms like X or Facebook can be leveraged to provide continuous, relevant learning opportunities beyond traditional classroom settings, addressing gaps in cybersecurity education (Le et al., 2019).
- Frequent cybersecurity events: Organising regular security training and conferences for all stakeholders, including students and senior management, and training on cyber ethics can enhance overall cybersecurity awareness and practices (Maranga and Nelson, 2019).

**Author Contributions**: Mouwers-Singh, C.: Conceptualisation, Writing-Original draft preparation, Methodology, Literature Review. Musikavanhu, T.B.: Reviewing and Editing, Writing-Original draft preparation, Methodology, Literature Review.

**Funding**: This research received no external funding.

**Conflicts of Interest**: The authors state that they have no conflicts of interest.

## References

Abawajy, J. 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), pp. 237-248.

AIICT Team. 2022. *What is cyber security awareness, and why is it important?* Australian Institute of ICT. [online] Available at: https://aiict.edu.au/blog/what-is-cyber-security-awareness-and-why-is-it-important/ [Accessed on 25 June 2023].

Al-Alawi, A. I., Al-Kandari, S. M. and Abdel-Razek, R. H. 2016. Evaluation of information systems security awareness in higher education: An empirical study of Kuwait University. *Journal of Innovation and Business Best Practice*, 2016, pp. 1-24.

Al-Alawi, A. I., Mehrotra, A. A. and Al-Bassam, S. A. 2020. Cybersecurity: Cybercrime Prevention in Higher Learning Institutions. In *Implementing Computational Intelligence Techniques for Security Systems Design* (pp. 255-274). IGI Global.

Alexei, L. A. 2021. Cyber security strategies for higher education institutions. *Journal of Engineering Sciences*, (4), pp. 74-92.

Alharbi, T. and Tassaddiq, A. 2021. Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), pp. 23.

Anderson, D., Abiodun, O. P. and Christoffels, A. 2020. Information security at South African universities—implications for biomedical research. *International Data Privacy Law*, *10*(2), pp. 180-186.

Chanani, U. L. and Wibowo, U. B. 2019. A learning culture and continuous learning for a learning organisation. *KnE Social Sciences*, pp. 591-598

Charandura. 2022. *Cybersecurity in the education industry*. SNG Grant Thornton. [online] Available at: https://www.grantthornton.co.za/Newsroom/cybersecurity-in-the-education-industry/ [Accessed on 17 June 2023].

Cheng, E. C. and Wang, T. 2022. Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), pp. 192.

CIUCHI, C. 2022. Developing a Comprehensive Model for Digital Lifelong Learning Using Cyber Resilience Framework. In *Proceedings of the International Conference on Cybersecurity and Cybercrime-2022* (pp. 105-112). Asociatia Romana pentru Asigurarea Securitatii Informatiei.

Cojocariu, A. C., Verzea, I. and Chaib, R. 2020. Aspects of Cyber-Security in Higher Education Institutions. *Innovation in Sustainable Management and Entrepreneurship: 2019 International Symposium in Management (SIM2019)* (pp. 3-11). Springer International Publishing.

Colwill, C. 2009. Human factors in information security: The insider threat–Who can you trust these days? *Information security technical report*, *14*(4), pp. 186-196.

Dioubate, B.M. and Daud, W.N., 2022. A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, 12(5), pp.1031-1093.

Dioubate, B. M., Norhayate, W. D. W., Anwar, Z. F., Fauzilah, S., Faiz, H. M. and Hai, L. O. 2023. The Role of Cybersecurity on the Performance of Malaysian Higher Education Institutions. *Jurnal Pengurusan*, 67, pp.1-12.

Fouad, N. S. 2021. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy, 6(2),* pp. 137-154.

Framework in Malaysia Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(5), pp. 1081-1093.

Gordon, S. and Ford, R. 2006. On the definition and classification of cybercrime. *Journal in computer virology*, 2, pp. 13-20.

Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K. and Nazeer, J. 2023. Cybersecurity in Universities: An Evaluation Model. *SN Computer Science*, *4*(5), p. 569.

Hijji, M. and Alam, G. 2022. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors, 22*(22), p. 8663.

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N. L. and Xu, X. 2023. The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Education and Information Technologies, 28*(1), pp. 439-470.

Interpol. 2021. Interpol's key insight into cybercrime in Africa. Interpol. Retrieved from: https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O. and Gale Vergara, R., 2022. A systematic literature review on cybercrime legislation. *F1000Research*, 11, p.971.

Le, H., Johri, A. and Malik, A. 2019. *Curating tweets: A framework for using Twitter for workplace learning*. ASEE Annual Conference proceedings.

Luiijf, E., Besseling, K. and De Graaf, P. 2013. Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6, 9*(1-2), pp. 3-31.

Maranga, M. J. and Nelson, M. 2019. Emerging issues in cyber security for institutions of higher education. *International Journal of Computer Science and Network*, *8*(4), pp. 371-379.

Miranda, M. J. 2018. Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2), pp. 5-10

Muniandy, L., Muniandy, B. and Samsudin, Z. 2017. Cyber security behaviour among higher education students in Malaysia. *J. Inf. Assur. Cyber Secur*, *2017*, pp. 1-13.

Mushwana, G. 2023. Digital skills development is critical to fight cybercrime. Engineering News. [online] Available at: https://www.engineeringnews.co.za/article/digital-skills-development-is-critical-to-fight-cybercrime-2023-05-23 [Accessed on 25 June 2023].

Ramalingam, R., Khan, S., and Mohammed, S. 2016. The need for effective information security awareness practices in Oman's higher educational institutions.

Ramdhani, A., Ramdhani, M. A. and Amin, A. S. 2014. Writing a Literature Review Research Paper: A step-by-step approach. *International Journal of Basic and Applied Science*, *3*(1), pp. 47-56.

Snyder, H. 2019. Literature review as a research methodology: An overview and guidelines. *Journal of business research, 104,* pp. 333-339.

Van Niekerk, B. 2017. An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication*, *20*, pp. 113-132.

Vasileiou, I. and Furnell, S. (Eds.). 2019. *Cybersecurity education for awareness and compliance*. IGI Global.

Xiao, H., Wei, H., Liao, Q., Ye, Q., Cao, C. and Zhong, Y. 2023. Exploring the gamification of cybersecurity education in higher education institutions: An analytical study. *SHS Web of Conferences*, *166*, p. 01036.

Zur, R. 2022. *Optimising Security awareness training with active learning*. Forbes.com. [online] Available at: https://www.forbes.com/sites/forbesbusinesscouncil/2022/02/18/optimizing-cybersecurity-awareness-training-with-active-learning/?sh=277d9f0c1a3a [Accessed on 25 June 2023].