Exploring Cybersecurity Implications in Higher Education

Nokuthaba Siphambili
University of Pretoria and Council for Scientific and Industrial Research (CSIR), South Africa

nsiphambili@csir.co.za

Abstract: With the rapid technological evolution and widespread integration of digital transformation in higher education institutions (HEIs), the educational landscape has undergone a shift in teaching methodologies and how content is delivered. The digitization of higher education has ushered in numerous benefits, enhancing accessibility, collaboration, and efficiency. However, this era of digitization of higher education also brings forth a plethora of cyber challenges. The objective of this paper is to comprehensively explore the cybersecurity landscape in the digital age, providing a critical analysis of prevailing cyber threats, emerging trends, and potential impacts on HEIs. Therefore, this study conducted a systematic literature review (SLR) using the PRISMA framework to assess the current cyber threats faced by higher education institutions. The findings of the study reflect on the challenges faced by higher education institutions in this digital age and present opportunities in strategies that may be adopted to protect HEI's systems from cyber threats.

Keywords: Cybersecurity, Cybersecurity Awareness, Higher Education Institutions (Heis), Digital Age, Online Learning

1. Introduction

The ongoing rapid technological changes have significantly transformed the way teaching is delivered in higher education institutions (HEIs). With the advent of major lockdowns due to the COVID-19 pandemic, digital teaching has emerged as a transformative force in higher education. This has revolutionized the way educators deliver learning content to students and the way students learn and engage with content. As higher education institutions increasingly leverage technology, cloud-based systems, and online platforms to deliver content, they must also be cautious of the inherent cybersecurity risks. The effect of the coronavirus has led to HEIs adopting online learning or hybrid learning scenarios. This has increased the need for HEIs to revise and step up the way they protect their data and systems. Jana et al. (2023) state that the digital transformation from traditional teaching 'chalk and board' approaches to a digitalized one offers exciting opportunities for the future of higher education. Yet, the challenges for advancement in the way content is delivered cannot be ignored. For example, the move to exploit the opportunities of digital spaces, raises the need for higher education institutions to improve their administrators', educators' and students' cyber hygiene through cybersecurity awareness campaigns that aim to make them aware of the implications of the ever-increasing cyber threats.

As higher education institutions started migrating their on-campus programmes to online platforms, they have also been faced with an increase in cyber threats. These include ransomware, distributed denial of service, data breaches and social engineering attacks. All these cyber threats call for higher education institutions to adequately protect their systems from any unauthorized access, usage, disclosure, modification, destruction, and deletion by threat actors. Therefore, this paper aims to explore the cybersecurity implications in the digital age, highlighting the vulnerabilities and risks faced by the higher education sector as they navigate the ever-evolving digital landscape. More than ever before, it is now essential for higher education institutions to ensure that their systems are well-protected from cyber threats. However, before this paper can discuss how this can be achieved, it is also important to note that the concept of cybersecurity has already been defined in other fields like information security or computer security. Yet, to the author's knowledge and up until now, there is still no widely accepted definition of cybersecurity in the context of higher education institutions. The author believes that the HEI environment is quite unique in its way and therefore demands that the concept of cybersecurity be revised and defined to fit its context.

2. Definition

Several authors have different definitions of cybersecurity (Jana et al., 2023; Taherdoost, 2022; Antunes et al., 2021; Hamdani et al., 2021; Thakur et al., 2015). In some cases, it is used interchangeably with information security (Jana et al., 2023; Taherdoost, 2022). Yet in other cases, it is discussed as a different concept to information security (Antunes et al., 2021). Information security, also known as info sec deals with protecting information in all forms, whether in physical or digital form and cybersecurity focuses on protecting information and systems from any cyber threats. The author believes that these two, i.e., info security and cybersecurity are somehow similar yet unique in various aspects. However, this paper focuses on cybersecurity. Therefore, this section continues to compare some of the definitions of cybersecurity that are found in the literature and ends by contextualizing it to the HEI environment."

According to Thakur et al. (2015), cybersecurity is defined as the process of safeguarding against unauthorized access, use, disclosure, alteration, and destruction of computer systems, networks, and data. This is a good definition because it covers systems, networks and the data they transmit or process. However, it does not consider unauthorized denial of service by a malicious insider. For example, in the context of higher education, an authorized student who is ill-prepared for an exam may easily execute a freely available distributed denial of service attack (DDOS) that aims to compromise the availability of a system (Gupta & Badve, 2017) on the exam server and deny other students who have prepared a chance to write an exam. Therefore, this definition can be improved as follows; cybersecurity is defined as the process of safeguarding against denial of a service, unauthorized access, use, disclosure, alteration, and destruction of computer systems, networks, and data.

Hamdani et al. (2021) define cybersecurity as technology that prevents hostile parties from exploiting and misusing digital assets by preventing unauthorized access. This definition adds the element of 'a hostile party', 'misuse' and 'preventing authorized access' to the one of (Thakur et al., 2015). Therefore, by taking a combination of two definitions, one can arrive at a more encompassing definition. This can be stated as follows: a process of safeguarding against hostile parties exploiting weaknesses in systems, networks and applications to purposely prevent authorized access from other authorized users; carry out unauthorized access, use, disclosure, alteration, and destruction of the data they store, collect, transmit or process. Though the combination of the two definitions seems to be all-encompassing, the author of this paper has purposely chosen to define cybersecurity as the process of protecting HEI data, systems and networks from unauthorized users by preventing them from accessing, using and disclosing their weaknesses. This definition contextualizes cybersecurity to the HEI environment. An example of cybersecurity in higher education is protecting sensitive research data from unauthorized access or theft. This includes implementing encryption protocols and firewalls to safeguard valuable information from potential cyber threats. Additionally, cybersecurity also involves educating students and staff about the best practices for creating strong passwords and being vigilant against phishing attempts to prevent unauthorized access to personal accounts and sensitive data.

This research aims to investigate the implications of cybersecurity in digital learning, looking at the challenges and opportunities in higher education. This will be done following the methodology in the next section.

3. Methodology

A systematic review of the literature was carried out that focused on finding the existing literature on cybersecurity implications. The following research question guided the study*: "What are the cybersecurity implications of digital teaching in higher education?".* The Preferred Reporting Items for Systematic and Meta-analysis (PRISMA) framework was used to target publications between 2019 and 2023 with search terms ("*cybersecurity*" OR "*information security*" AND "*implication*" AND "*digital*" OR "*online" learning*). The following databases were used Scopus, Elsevier, Google Scholar, Taylor and Francis Online for comprehensive results.

The articles were screened through the process of reading abstracts and irrelevant articles were eliminated as shown in Table 1 below. After the inclusion and exclusion criteria were applied, 70 publications were excluded and 25 publications were found to be eligible for the full review as illustrated in Annexure A.

Table 1: Inclusion and Exclusion Criteria

Inclusion
Articles published between 2019 and 2023.
Articles that discuss online learning and cybersecurity implications.
Exclusion
Articles not written in English.
Articles that are not accessible.
Articles that are duplicates.

4. Findings

4.1 Cyberthreats

Higher education institutions face challenges from various cyber threats, such as data breaches, denial of service (DoS), malware attacks, malicious insiders, external users, and cloud providers (Alexei and Alexei, 2021b). Broadhurst et al., (2019) examine how criminals target students through spam emails that contain phishing attacks to deliver malware and ransomware and obtain personal information without authorization for identity theft. For example, students often receive spam emails in the form of discounts and rewards. Sharma (2021) states how malware affects higher education institutions, causing data loss and the inability to access some services. Cyber criminals use phishing emails to target their victims by sending an email to a targeted victim in hopes that the victim will click on the link. To ensure that their systems follow the confidentiality, integrity and availability (CIA) triad, academic institutions ensure that they can manage cybersecurity threats with online learning (Merchan-Lima et al., 2021; Sekgololo, 2021). As a result, an organization is guaranteed to be able to identify vulnerabilities, address these risks, and gauge the impact. Threat actors target HEIs using social engineering to find vulnerabilities they will exploit to gain access to data and information being handled by HEIs (Merchan-Lima et al., 2021; Turnbull et al., 2021; Guangul et al., 2020).

4.2 Interest in Personal Information

As a result of the COVID-19 pandemic, learning has changed as higher academic institutions now deliver educational content using the most up-to-date technologies using computers, software, the Internet, and other applications (El Firdoussi et al., 2020). According to Alexei and Alexei, (2021b), criminals are now interested in collecting students' personal information, which they then utilize in phishing attempts due to hybrid learning. Due to the personal information and data they hold including identity numbers, staff and student intellectual property, higher education institutions are targets of cybercrime (Alexei, 2021a; Fouad, 2021; Fishman et al., 2018). Due to the shift to hybrid learning, these institutions are now targets, which raises the danger and volume of cybersecurity incidents in the sector (Ulven & Wangen, 2021). Due to the shift in teaching methodologies, HEIs are handling more sensitive data and information of students and staff resulting in threat actors aiming to gain access to this data and information (Khan et al., 2023).

4.3 Human Error

Humans are the main causes of data breaches as it is easy to make errors, such as an employee working in HEIs as a part-time lecturer, they can easily be acknowledged (Amoresano & Yankson, 2023; Othmana et al., 2020). According to Maranga and Nelson (2019), higher education institutions in Kenya must deal with issues that include insecure personal areas where employees, teachers and students are allowed to bring their own devices. More than 25% of phishing attacks in the UK's education sector in 2020 targeted university platforms, email, and video conferencing software (Amoresano & Yankson, 2023; Alexei, 2021a). Due to changes in teaching methods, the majority of employees now work from home, which calls for caution because people can become victims of data breaches (Georgiadou et al., 2022).

In addition, Netshakhuma (2023) claims that higher education's cybersecurity policies and standards are not up to par and that a framework for managing cybersecurity is lacking. Institutions must overcome this problem by taking all necessary security precautions to ensure that any device that accesses their network is secure and does not pose any threat. According to the article by Majola (2020), Lincoln College in the United States was hit by a ransom attack in May 2022, the University of Mpumalanga has been a victim of cyber breaches with bank account attacks, and a first-year student at the University of Johannesburg had their personal information sent to all students by mistake.

4.4 Skill Shortages

Cybersecurity is a growing field where management is tasked with ensuring that they protect their systems from any cyber-attacks. There are skills shortages as HEIs continuously face challenges with finding skilled people to fill cyber-security-related positions in the higher education sector and shortages of cybersecurity skills in the education sector in the European educational sector (Blaic, 2021). Due to the lack of skilled professionals in HEIs, not all students are trained or taught how to be safe online, which can result in the students being victims of cyber-attacks or incidents. Most employees are trained in cybersecurity and do not focus on why they should learn which results in employees being unable to assess risks where there is a need for inclusivity of all employees in organizational security (Amoresano & Yankson, 2023; Zwilling, 2022).

5. Recommendations

5.1 Cyber-Hygiene

HEIs should ensure that there is cybersecurity training and awareness by spending more time on cybersecurity (Gearhart, Abbiatti & Miller, 2019). This will help staff, students and faculty recognize the risks and potential threats associated with digital platforms so that academic institutions minimize cybersecurity vulnerabilities such as data loss and unauthorized access to their information and data. For example, there could be a compulsory course for students focusing on cyber awareness in higher education institutions. To stay ahead of new cyber risks, institutions must continually assess their practices, learn from incidents, and adapt their approaches. Having robust cybersecurity protocols will help ensure that there is a regular assessment of the institution's security and ensure that their data and networks are encrypted to prevent unauthorized access. They must ensure they have strong cybersecurity policies, routinely evaluate their security and encrypt their network and data to prevent unauthorized access. HEIs should invest in advanced technologies such as Intrusion Detection and Prevention Systems (IDS/IPS), web application firewalls (WAF) and Anti DDoS systems (ADS) (Merchan-Lima et al., 2021). Organizations should ensure that data at rest is encrypted by following existing IT policies and there is continuous monitoring of networks and systems (Alwahaibi et al., 2022)

5.2 Hiring Talent and Upskilling

There is a shortage of cybersecurity professionals in the world and the higher education sector is no exception. Hiring a qualified professional will help guide how content should be delivered to students and staff during training and awareness programmes. Students or graduates can be hired to be trained and skilled in the field and the existing employees can also be upskilled where the institutions pay for the certification of the employees who will be upskilling or training to be professionals in the field. Upskilling ensures that users are aware of risk which results in the reduction of risky behaviors that lead to users falling victim to cyber crimes (Moustafa et al., 2021)

5.3 Collaboration

Higher education institutions should collaborate to find solutions and pool resources to improve cybersecurity measures. This includes collaboration with other institutions, industry professionals, and cybersecurity specialists. For example, a partnership with the University of Cape Town, a member of the Forum of Incident Response and Security Teams (FIRST), which is a global forum of incident response and security teams will help other HEIs know how to respond to incidents and threats. Additionally, academic institutions can perform penetration tests to assess their security systems. These tests can help identify vulnerabilities and risk mitigation strategies. Furthermore, this opportunity allows these institutions to learn from experts in the field, cybersecurity specialists, or other higher education institutions. These suggestions can help higher education institutions navigate the world of online learning while successfully addressing cybersecurity issues.

5.4 Have a Culture That Supports Cybersecurity

Organizations should have a culture that supports cybersecurity to ensure that they protect their systems and information against cyber attacks (Kundy & Lyimo, 2019). This will ensure that people are aware of these cyber threats due to the fact that humans are the main causes of data breaches; therefore, the chances of these attacks happening will be lesser as the management will be leading by example. To respond to these cybersecurity threats, assign a cybersecurity responsibility to the Chief Information Officer (CIO), who will ensure that there are people responsible for cybersecurity (Gearhart et al., 2019). If management is assigned the role of being cyber warriors, employees and students will be motivated to take part in training and awareness. According to Chapman (2019), students should get basic information technology and network infrastructure knowledge so that they learn how to ensure that they follow the information security standards set by the institutions. This will help ensure that every student in higher education has a basic understanding of what cybersecurity is and how to ensure that they stay safe online.

6. In Conclusion

The digital age has created transformative opportunities for higher education institutions, revolutionizing how knowledge is shared, accessed, and absorbed. However, these opportunities are not without their accompanying challenges, particularly in the realm of cybersecurity. The main findings of this study showed that there is an increase in cyber threats such as data breaches, interest in personal information from threat actors, skill shortages and human errors. Therefore, this study recommended that HEIs must ensure that their systems are protected against cyber-attacks. Furthermore, this study provided recommendations that will ensure that HEIs stay prepared against cyber related threats. They must consistently invest in technology and train their employees and students to ensure that their institutions are secure against cyber threats. Higher education institutions must educate students, keep up with cyber threats and ensure that unauthorized users cannot access their data as technology is always changing as a result of new advances (Thakur et al., 2015).

Acknowledgement

The author would like to thank the Council for Scientific and Industrial Research (CSIR) for financial support.

References

Alexei, A. (2021a) "*Network Security Threats to Higher Education Institutions".* Budapest, Hungary, Central and Eastern European eDem and eGov Days. https://doi.org/10.24989/ocg.v341.24

Alexei, A. and Alexei, A. (2021b) "Cyber security threat analysis in higher education institutions as a result of distance learning" International *Journal of Scientific and Technology Research,* Vol 10, No. 03, pp 128-133.

Alwahaibi, A., Bin, W., Hassa, W., Basri, W., Wan Ismail, W.B. and Almamari, M., 2022. A systematic literature review on its security standards for higher education institution. *Journal of Tianjin University Science and Technology,* 55(6), pp. 194- 213.

Amoresano, K. & Yankson, B., 2023. Human Error-A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *HOLISTICA–Journal of Business and Public Administration,* 14(1), pp. 110-132

Blaic, B. J. (2021) "The cybersecurity labor shortage in Europe: Moving to a new concept for education and training", Technology *in Society*, Vol 67, No. 101769, pp 1-13.

Broadhurst, R. G., Skinner, K., Sifniotis, N. and Matamoros-Macias, B. (2019) "Phishing and cybercrime risks in a university student community", International *Journal of Cybersecurity Intelligence & Cybercrime*, Vol 2, No. 1, pp 4-23.

Chapman, J. (2019) "*How Safe is Your Data?: Cyber-security in Higher Education* "(Vol. 12, pp. 1-6). Oxford, UK: Higher Education Policy Institute.

El Firdoussi, S., Lachgar, M., Kabaili, H., Rochdi, A., Goujdami, D. and El Firdoussi, L. (2020), "Assessing distance learning in higher education during the COVID-19 pandemic" *Education Research International*, Vol *2020*, pp.1-13.

Fishman, T. D., Clark, C. and Grama, J. L. (2018), [online]. Deloitte. https://www2.deloitte.com/za/en/pages/public-sector /articles /Elevating_cybersecurity _on_the_ higher _education_leadership_agenda.html.

Fouad, N. S. (2021) "Securing higher education against cyber threats: from an institutional risk to a national policy challenge", Journal *of Cyber Policy, Vol* 6, No. 2, pp.137-154.

Gearhart, G.D., Abbiatti, M.D. and Miller, M.T. (2019) "Higher education's cyber security: Leadership issues, challenges and the future", *International Journal on New Trends in Education and Their Implications*, Vol *10*, No. 2, pp.11-18.

Georgiadou, A., Mouzakitis, S. and Askounis, D., 2022. Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *35*(2), pp.486-505.

Guangul, F.M., Suhail, A.H., Khalit, M.I. and Khidhir, B.A., 2020. Challenges of remote assessment in higher education in the context of COVID-19: a case study of Middle East College. *Educational assessment, evaluation and accountability*, *32*, pp.519-535.

Khan, N. A., Brohi, S. N. & Zaman, N., 2023. Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. *TechRxiv,* pp. 1-6.

Kundy, E.D. and Lyimo, B.J. (2019) "Cyber Security Threats in Higher Learning Institutions in Tanzania, A Case of the University of Arusha and Tumaini University Makumira", Olva *Academy–School of Researchers*, Vol *2*, No. 3, pp.1-38.

Hamdani, S.W.A., Abbas, H., Janjua, A.R., Shahid, W.B., Amjad, M.F., Malik, J., Murtaza, M.H., Atiquzzaman, M. and Khan, A.W. (2021), "Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons", ACM *Computing Surveys (CSUR)*, Vol *54, No. 3*, pp.1-36.

Jana, P., Banerjee, D., Das, K., Maity, S., Sarkar, A. and Samanta, S. (2023), "Cyber Security: Trends and Appraisal on Threats, Attacks, and Security Models", In *Streamlining Organizational Processes Through AI, IoT, Blockchain, and Virtual Environments*, pp. 135-155. IGI Global.

Majola, G.(2022) "*IOL", [online],* https://www.iol.co.za/business-report/economy/cyber-security-universities-under-fire-42481925-60dc-439c-86a1-13eabd30121c.

Maranga, M. J. and Nelson, M. (2019) "Emerging issues in cyber security for institutions of higher education", *International Journal of Computer Science, Vol* 8, No. 4, pp. 371-379.

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G. and Quiroz, D., 2021. Information security management frameworks and strategies in higher education institutions: a systematic review. *Annals of Telecommunications*, *76*, pp.255-270.

Netshakhuma, N. S. (2023)" Cybersecurity management in South Africa", *IGI Global,* pp 1-16.

Sekgololo, J. (2021) "*Mail&Guardian",* [online].https://mg.co.za/thoughtleader/opinion/2021-06-09-cybersecurity-e-learning-and-the-rise-of-online-student-protests/.

Othmana, Z., Rahimb, N. & Sadiqc, M., 2020. The human dimension as the core factor in dealing with cyberattacks in higher education. *International Journal of Innovation, Creativity and Change,* 11(1), pp. 1-19.

Sharma, A. (2021) "Review on Major Cyber security Issues in Educational Sector", *International Journal of Computer Sciences and Engineering, Vol 9*, No. 12, pp. 26-29.

Taherdoost, H. (2022) "Cybersecurity vs. Information Security" *Procedia Computer Science,* Vol215, pp. 483-487.

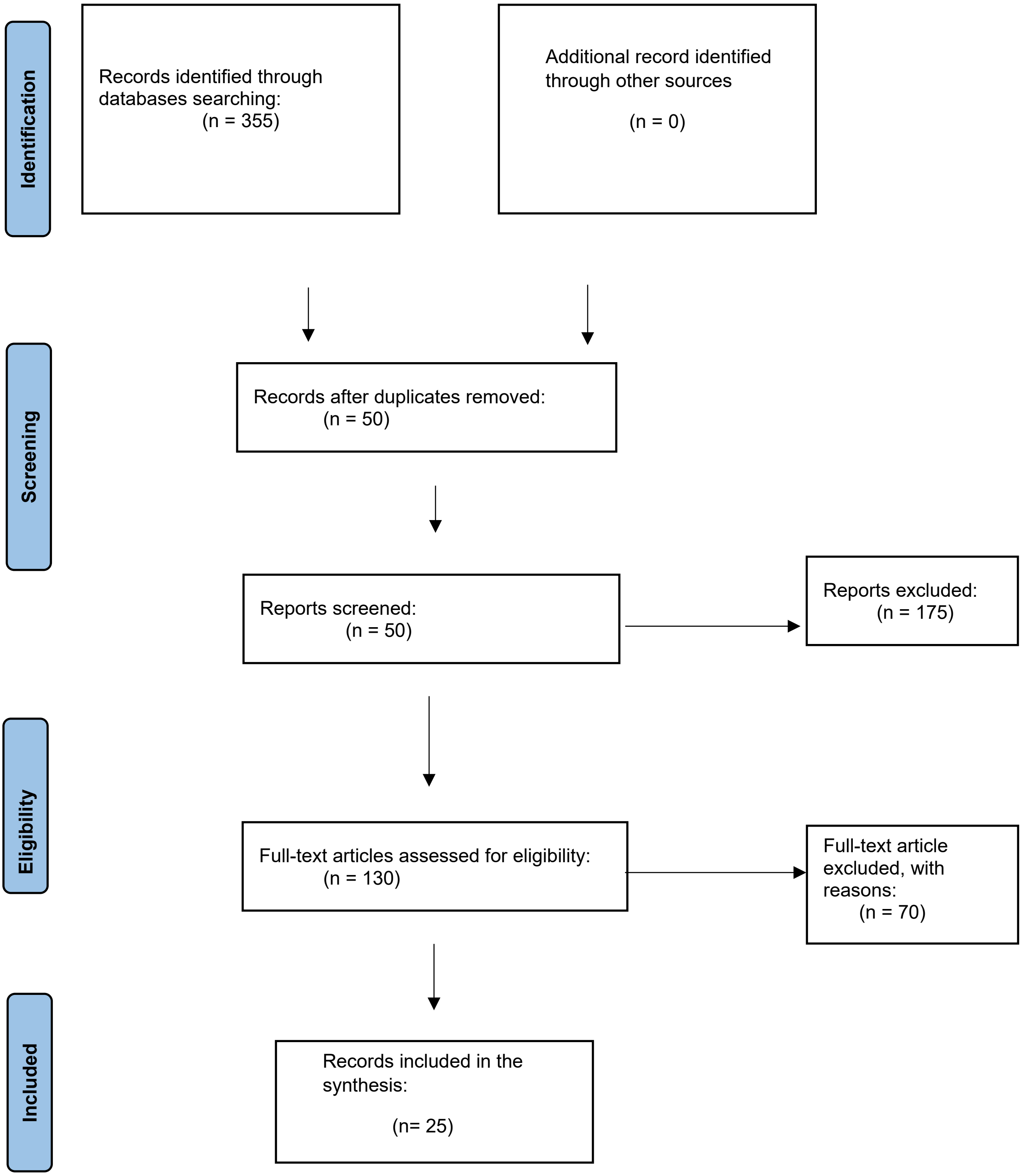
Thakur, K., Qiu, M., Gai, K. and Ali, M.L. (2015)" An investigation on cyber security threats and security models" Paper presented at the 2nd international conference on cyber security and cloud computing, USA, pp. 307-311 November 2015.

Turnbull, D., Chugh, R. and Luck, J., 2021. Transitioning to E-Learning during the COVID-19 pandemic: How have Higher Education Institutions responded to the challenge?. *Education and Information Technologies*, *26*(5), pp.6401-6419.

Ulven, J.B. and Wangen, G. (2021) "A systematic review of cybersecurity risks in higher education", *Future Internet*, Vol 13*, No.* 2, pp 1-39.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N., 2022. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), pp.82-97.

Appendix A: PRISMA flowchart


Identification
Records identified through databases searching: (n = 355)
Additional record identified through other sources (n = 0)
Screening
Records after duplicates removed: (n = 50)
Reports screened: (n = 50)
Reports excluded: (n = 175)
Eligibility
Full-text articles assessed for eligibility: (n = 130)
Full-text article excluded, with reasons: (n = 70)
Included
Records included in the synthesis: (n= 25)