Journal of Communication in Scientific Inquiry
Volume 6 Issue 1, June 2024 [47-55]

Challenges and Opportunities of Cybersecurity Education for Non-technical Majors

Norlizawati Ghazali[1,2], Ina Suryani[3,*] and Syed Zulkarnain Syed Idrus[1]

[1]Fakulti Perniagaan dan Komunikasi, Universiti Malaysia Perlis
[2]Universiti Teknologi MARA Cawangan Perlis, Malaysia
[3]Centre of Excellence for Unmanned Aerial Systems (COEUAS), Universiti Malaysia Perlis, Malaysia

*Corresponding Author: inasuryani@unimap.edu.my

Received 5th April 2024, Revised 22nd May 2024, Accepted 26th June 2024

ABSTRACT

Cybersecurity is fast becoming a crucial area of study due to the advancement of digital technology. As cybersecurity impacts all digital technology users, there is a pressing need for educating users on this issue. Moreover, the risk of falling victim to cyber threats is far more eminent in non-technical background users. Thus, this study focuses on the need for cybersecurity education towards non-technical majors in university, as an effort to address this problem. Through analysis of previous literatures, this paper highlights the possible challenges and opportunities in teaching cybersecurity for non-technical majors. This could provide valuable insights into the digital literacy gap for non-technical majors. The relevance of this study lies in its potential to enhance cybersecurity awareness and promote a safer digital environment.

Keywords: Cybersecurity education, digital literacy, non-technical majors, cybersecurity awareness

1. INTRODUCTION

In the era of digital globalisation, cybersecurity becomes an overriding concern that touches the life of everyone from individuals and corporations to governments. Our increasing dependence on a digital world also increases our vulnerabilities to the cyber threats that compromise our privacy, our economic stability, and our national security. Malaysia itself is a classic case in this scenario. In 2023 alone, there are 5917 cyber incidents that have been reported to the Malaysia Computer Emergency Response Team/MyCERT (MyCERT, 2023). Cyber security incidents is increasing and affecting many groups (Buja et. al., 2021). Cybersecurity threats that span different categories such as intrusion attempts, malicious codes, spam and fraud, indicate the urgency for cyber security awareness campaigns towards the public.

The apparent prevalence of cyber threats has exposed an alarming lack of cyber security knowledge among non-technical majors in the workforce (Almoughem, 2023). Without these basic skills, they are also left vulnerable when it comes to recognising and protecting against cyber risks, putting their organisations at risk of breaches with far-reaching implications. Non-technical employees have difficulty spotting phishing, keeping secure passwords, and data protection best practices in professional settings (Cravens & Resch, 2023). Non-technical majors often lack strong cybersecurity hygiene relevant to the general population and are significantly lacking in practical cybersecurity understanding compared to their technical peers (Oliveira et al., 2023). Moreover, this does not only endanger personal data but also affects the security systems of the enterprises they are employed in. Given the threats and uncertainties, it is important for universities to have more cybersecurity education for non-technical students to give them the necessary skills to interact with digital threats.

This responsibility extends to universities, as they play a pivotal role to ensure that cybersecurity proficiency is not only an exclusive skill reserved for technical majors. Non-technical majors, who face far more impending threats need to be considered in every cybersecurity embedded curriculum. Due to the fact that these students usually move on to positions exposed to cyber threats, they need to be able to protect their personal, and their employers data. They should have the acquisition of the correct security knowledge and the skills to avoid threats (Mountrouidou et al., 2018).

Existing works have shown that flexible, experiential ways of learning, like those used with liberal arts education intervention, can improve cybersecurity awareness and practice among non-technical students (Mountrouidou et al. 2018). Almost everyone, including students, is using electronic gadgets connected to internet such as smartphones, tablets and computer in their daily life (Mohd Nawi et. al., 2021). The Malaysia's New Economic Model highlights the importance to remain sustainable, where the present requirement is to be met without compromising the prosperity of future generation (Abd Rashid, Abd Rahim, & Noh, 2014, Ismail et. al., 2021). Alongside universities such as Universiti Teknologi Malaysia (UTM), Universiti Malaya (UM), and Multimedia University (MMU) have developed cybersecurity curricula that blend technical knowledge with essential soft skills. These programs cover a wide range of topics, from network security and cryptography to cybersecurity management and policy. Through the integration of cybersecurity training into general education, universities can facilitate a baseline level of cybersecurity awareness and knowledge for all students, irrespective of their program of study (Kraus et al., 2023). Such move not only unlock the immediate knowledge gap of cybersecurity, but also seed a cyber aware mentality ready for cybersecurity threat defence. Going forward, non-technical graduates that have received such education will be in a better position to identify and address cyber threats, effectively leveraging them as part of the security posture of their organisations (Kraus et al., 2023). Hence, it is crucial for universities to make cybersecurity an integral part of their academic curriculums for non-technical majors.

Thus, this paper aims to address this critical issue and bridge the knowledge gap by exploring the challenges and opportunities associated with cybersecurity education towards non-technical majors in university settings. While this paper provides a general perspective applicable to educational institutions worldwide, the insights and strategies discussed are not limited to any specific country, including Malaysia.

2. THE IMPORTANCE OF CYBERSECURITY EDUCATION FOR NON-TECHNICAL MAJOR

Cybersecurity issues affect everyone contrary to previously popular belief that it should only be dealt by those related in the IT industry only. In fact, it poses greater effect towards those in business, humanities and social sciences industry due to their susceptibility to cyber threats. Those working in these industries, are likely to be non-technical majors from universities. Their lack of ability to recognize, and effectively handle cyber threats makes them a more vulnerable group as compared to the more capable technical majors. Thus, including cybersecurity for non-technical majors is crucial due to the rising demand for cybersecurity (Mack et. al., 2020) and the significant impact of poor cybersecurity skills on organisations (Dupuis, 2017).

The growing importance of cybersecurity education, particularly for nontechnical majors, has been thoroughly documented. With the prevalence of digital technology in all spheres of human activity, proper cybersecurity can hardly be overemphasised. In many cases, sensitive data should be treated by majors professionally. For instance, HR specialists deal with confidential records, while financial consultants are responsible for the accounts of the clients. The same applies to research which also require management policies related to cybersecurity at some point (Ahmadi, Jano, & Khamis, 2016). Without proper cybersecurity training, workers in these important roles could cause data breaches inadvertently (Rawindaran et. al., 2022). However,

non-technical skills are often undervalued in cybersecurity training, limiting career progression into roles like cybersecurity advocates for professionals from diverse backgrounds (Haney & Lutters, 2021)

Several studies underline the issues and the potential related to introducing cybersecurity education into the university curricula, especially for nontechnical majors (Carlton, Levy & Ramim, 2019, Peker et. al. 2018, Peker et. al. 2016) . This review is thus engaged in such a discussion, being based on different studies dealing with the current state of cybersecurity education and potential pathways towards increasing the level of effectiveness for such inclusion within the general education in university.

3. CHALLENGES IN TEACHING CYBERSECURITY TO NON-TECHNICAL MAJORS

3.1 Lack of Fundamental Knowledge

Teaching cybersecurity to non-technical majors poses challenges due to the lack of fundamental knowledge in this field (Diawati , 2023, Kilhoffer et. al., 2023, Syarova & Toleva-Stoimenova, 2023). Many non-technical majors enter university with little or no knowledge of cybersecurity concepts. This situation is worsen as research indicates that despite the increasing threat of cyber-attacks, information security does not hold the necessary importance in the curricula of non-IT majors (DeBello et. al., 2022). This foundational gap consequently places them at a massive disadvantage because no grounding would have enabled a quick grasp and understanding of higher and more complex principles of cybersecurity. As Almoughem (2023) highlighted, it is this very demographic that is most likely to fall prey to cyber threats due to a lack of knowledge concerning basic practices of cybersecurity.

3.2 Poor Cyber Hygiene Practices

One of the most critical challenges is the incapability of cybersecurity hygiene of non-technical majors as they are not exposed to formal cybersecurity education (DeBello et. al., 2023). For example, according to Cravens and Resch (2023) and Oliveira et al. (2023), non-technical workers often encounter difficulties with detecting phishing, managing secure passwords, and, in general, following data protection practices. For this reason, the user is not only putting personal information at risk but also that of an organisation, leading to security risks on networks and systems which host the important data of an organisation.

3.3 Limited Access to Tailored Educational Resources

Previous research highlights the importance of integrating cybersecurity into curricula for all disciplines (Syarova & Toleva-Stoimenova, 2023) and emphasises the need for cross-disciplinary training to meet current and future educational requirements (Martin & Collier, 2020). However, many universities often lack the resources to provide specialised cybersecurity training tailored for non-technical majors. Mountrouidou, Li, and Burke (2018) highlights that while larger research institutions may have the infrastructure to offer comprehensive cybersecurity programs, smaller liberal arts colleges and universities often struggle to integrate such courses due to limited funding and faculty expertise. Despite the growing number of cybersecurity educational resources available, Langner et. Al. (2022) claims that there is a lack of teacher perspective on their effectiveness and dissemination, hindering optimal use in classrooms. Additionally, the absence of guidelines for cybersecurity education outside technical fields leaves individuals in non-technical majors, such as high school students or those in other disciplines, without structured training on cybersecurity and privacy issues that are increasingly relevant in daily life (DeBello et. al., 2023).

3.4 Resistance to Incorporating Cybersecurity into General Curriculum

Initially, research has primarily focused on infusing cybersecurity topics into existing courses rather than developing a comprehensive cybersecurity awareness framework (Khader et al., 2021). As a result, integrating cybersecurity education into the general curriculum for non-technical majors is met with resistance. Besides, many academic departments view cybersecurity as a highly specialised field that does not directly apply to their discipline. This perception hinders the inclusion of cybersecurity modules in general education courses. Mountrouidou, Li, and Burke (2018) note that overcoming this resistance requires demonstrating the interdisciplinary nature of cybersecurity and its relevance across various fields of study.

4. OPPORTUNITIES IN TEACHING CYBERSECURITY TO NON-TECHNICAL MAJORS

4.1 Integration of Experiential Learning Modules

It is crucial to integrate experiential learning modules to teach cybersecurity to non-technical majors Research indicates that experiential learning modules can be particularly effective. Mountrouidou, Li, and Burke (2018) have demonstrated that incorporating hands-on, practical exercises into the curriculum can significantly enhance students' understanding and retention of cybersecurity concepts. In this era of uncertainties, learning is about having the knowledge and skills that are necessary for learners to understand, discuss, reflect and use multiple representations of texts to participate effectively in a variety of formal and social situations (Behak et.al., 2021). Moreover, incorporating game-based learning methods (Zubir, Suryani, & Ghazali, 2018), such as the use of video games for AI security education, can make cybersecurity education more engaging and relevant (Jin et al., 2018; Arai, 2024). Additionally, the development of authentic cybersecurity learning experiences, such as playable case studies, can provide students with immersive and experiential learning opportunities that simulate real-world cybersecurity challenges (McDonald et al., 2019). Furthermore, the integration of virtual reality into experiential education can enhance self-efficacy and learning motivation, contributing to a more effective educational experience (Hsiao, 2021).

4.2 Development of Interdisciplinary Courses

The construction of courses that integrate more than one subject (interdisciplinary courses) is also another opportunity for effective cybersecurity education. Through this integration, students will be able to have a broader and more meaningful understanding of cybersecurity in their primary studies (Kraus et al., 2023). Through this integration, a more relevant approach to cybersecurity can be established, resulting in a more lasting cybersecurity awareness that students can adopt into their working environment.

Nonetheless, this integration is not exclusive to courses. Sharevski, Trowbridge, and Westbrook (2018) suggested that integration within sub-disciplines can also be beneficial, such as the integration of cybersecurity with user interaction design, which could result in a more holistic approach. Furthermore, collaboration can also be appreciated within the teaching methods. Students can engage in peer learning while experimenting with real world scenarios and projects in a collaborative teaching and learning environment. The incorporation of integration and collaboration, as highlighted above, can enhance students' understanding and application of cybersecurity (McNulty & Kettani, 2020).

4.3 Use of Online Education Platforms

The use of online education platforms presents a viable solution to the challenge of limited resources in teaching cybersecurity to non-technical majors. The utilisation of online courses and virtual labs helps universities in providing accessible and flexible cybersecurity training. The effectiveness of online cybersecurity education has been highlighted in several studies. For instance, a case study analysis emphasizes the need for continuous updates and interactive engagement to keep students motivated and informed about the latest cybersecurity threats and practices (Erendor & Yildirim, 2022).

Additionally, the integration of learning management systems (LMS) with cybersecurity training activities can streamline the educational process and make it more efficient for both instructors and students. This integration can facilitate automated activity management and provide a cohesive learning experience (Beuran et al., 2019). Moreover, incorporating hands-on learning through virtual labs can significantly enhance students' practical skills and their ability to understand complex cybersecurity concepts. The use of virtual laboratories has been proven to increase the efficiency of the educational process and improve the professional competencies of future cybersecurity professionals (Buriachok et al., 2020). These approaches not only address the resource constraints but also ensure that non-technical majors receive a comprehensive and practical education in cybersecurity.

4.4 Collaboration with Industry Experts

Collaborating with industry experts can also enhance the quality and relevance of cybersecurity education. Industry professionals can provide valuable insights into current cybersecurity trends and practices, ensuring that the curriculum remains up-to-date with industry standards and practices (Sarker et al. 2021). Besides, industry collaboration can also help in identifying the essential skills required in the field, such as systematic thinking, collaboration, strong communication, continuous learning, and a sense of civic duty, which are crucial for future cybersecurity professionals (Blažič, 2021). Additionally, through collaboration with industry partners, non-technical majors can enhance cybersecurity research, education, and the dissemination of best practices (Maphosa, 2024) and get the exposure to industry infrastructure, platforms, access to experts, and technical knowledge, enriching their learning experience (Kaicker et. al, 2023).

5. CONCLUSION

It is hoped that the insights from this paper might be helpful for institutions that are discussing and planning for future cybersecurity education. The present researchers show that the integration of cybersecurity education for non-technical majors presents both significant challenges and remarkable opportunities that need to be carefully navigated. It is believed that as digital technology continues to advance, the risk of cyber threats grows. Previous research highlights that there is a genuine need to support universities that are designing and offering cybersecurity education.

Despite the challenges and opportunities in the field of cybersecurity education for non-technical majors, there are other perspectives that need to be addressed. It is imperative for educational institutions and universities to equip all students, regardless of their major, with the knowledge and skills necessary to navigate this landscape safely. For instance, by incorporating a combination of technical skills, domain-specific knowledge, and social intelligence, educators can better prepare students for successful cyber performance Dawson & Thomson (2018). Moreover, it is crucial to integrate theoretical, technical, and non-technical skills into cybersecurity training curricula to address the diverse needs of learners (Bjerrum et al., 2018). Additionally, by

leveraging active learning activities (Arif, Abd Aziz, & Abdurakhmonovich, 2024; Srivatanakul & Annansingh, 2021) and emphasising the need for continuous faculty development and student support in online teaching (Clune et al., 2022) universities can enhance students' problem-solving abilities and cybersecurity skills.

Future research should refine the cybersecurity education for non-technical majors and tackle the identified challenges and opportunities. It is important that universities must overcome the resistance to incorporating cybersecurity into general education and invest in tailored educational resources that address the unique needs of non-technical majors. This entails investigating effective pedagogical strategies, assimilating the curriculum with established educational frameworks, and ensuring its relevance to industry demands. Moreover, regular assessments are essential to verify the curriculum's efficacy and its contribution to the anticipated outcomes.

Looking forward, the successful implementation of comprehensive cybersecurity education for non-technical majors can foster a culture of cybersecurity awareness that extends beyond the academic environment. As discussed before, universities can start by leveraging experiential learning modules, interdisciplinary courses, online education platforms, and industry collaborations. Besides, a robust framework or curriculum can be created to not only enhance the digital literacy of non-technical students but also prepare them to contribute effectively to their professional fields. As future employees, these students will carry forward the principles and practices of cybersecurity (Ahmad, Rahim, & Ahmad, 2021). This will also strengthen the overall security posture of their organisations and contribute to a safer digital society.

In conclusion, cybersecurity education for non-technical majors is essential in today's digital age. By incorporating a blend of technical and non-technical skills, active learning methods, and raising awareness about cybersecurity, individuals from diverse backgrounds can be better prepared to contribute effectively to the cybersecurity workforce.

ACKNOWLEDGEMENTS

My heartfelt thanks to the Ministry of Higher Education Malaysia for their generous sponsorship (SLAB) and support, without which this research would not have been possible. My deepest gratitude to my supervisor, Ass. Prof. Dr. Ina Suryani and my co-supervisor, Ass. Prof. Dr. Syed Zulkarnain for their invaluable guidance, support, and encouragement throughout this research.

REFERENCES

Abd Rashid, S., Abd Rahim, I. S., & Noh, N. I. M. (October, 2014). Aligning and Giving Meanings On Student Learning: A UniMAP Journey Facing New Challenges. In proceeding for *Malaysia University Conference Engineering Technology*.

Ahmad, N., Rahim, I. S. A., & Ahmad, S. (2021, July). Designing effective online assessment implementation strategies for tertiary language courses-narratives on preliminary overview of challenges. In *AIP Conference Proceedings* (Vol. 2347, No. 1). AIP Publishing.

Ahmadi, N. A., Jano, Z., & Khamis, N. (2016). Analyzing crucial elements of research data management policy. *International Business Management*, *10*(17), 3847-3852.

Almoughem, K. A. (2023). The Future of Cybersecurity Workforce Development. Academic Journal of Research *and Scientific Publishing. Vol*, *4*(45).

Arai, M., Tejima, K., Yamada, Y., Miura, T., Yamashita, K., Kado, C., ... & Hanaoka, G. (2024). REN-AI: A Video Game for AI Security Education Leveraging Episodic Memory. *IEEE Access*.

Arif, M., Abd Aziz, M. K. N., & Abdurakhmonovich, Y. A. (2024). Trend Strategy to Prevent Bullying in Islamic Boarding Schools (Pesantren). *Jurnal Ilmiah Peuradeun*, *12*(2), 639-670.

Behak, F. P., Mahir, N. A., Abd Hamid, Y. E., Selamat, S., Ali, S. M., Darmi, R., ... & Sidek, H. (2017). Exploring the use of multiliteracies project approach to enhance employability skills among Malaysian university graduates. *IJAEDU-International E-Journal of Advances in Education, 3*(8), 235-242.

Beuran, R., Tang, D., Tan, Z., Hasegawa, S., Tan, Y., & Shinoda, Y. (2019). Supporting Cybersecurity Education And Training Via LMS Integration: CyLMS. *Education and Information Technologies*, 24, 3619-3643.

Bjerrum, F., Thomsen, A. S. S., Nayahangan, L. J., & Konge, L. (2018). Surgical simulation: current practices and future perspectives for technical skills training. *Medical teacher*, *40*(7), 668-675.

Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?. *Education and information technologies*, *27*(3), 3011-3036.

Buja, A. G., Wahid, S. D. M., Rahman, T. F. A., Deraman, N. A., Jono, M. N. H. H., & Aziz, A. A. (2021). Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly. *International Journal of Advanced Technology and Engineering Exploration, 8*(76), 511.

Buriachok, V., Korshun, N., Shevchenko, S., & Skladannyi, P. (2020). Application of NI Multisim Environment in the Practical Skills Building for Students of 125 "Cybersecurity" Specialty. *Cybersecurity*, 1, 159-169.

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & Computer Security*, *27*(1), 101-121.

Clune, M., Charlton, A., Kam, M., Jowsey, T., Cosignani, D. R., & Singleton, R. (2022). Strengthening online teaching capability: Medical and health sciences faculty development. *ASCILITE Publications*, e22029.

Cravens, D., & Resch, C. (2023, October). Comparison of Password Hygiene for Computer Science and Non-Computer Science Undergraduates. In *Proceedings of the 24th Annual Conference on Information Technology Education* (pp. 112-117).

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in psychology*, *9*, 744.

DeBello, J. E., Schmeelk, S., Dragos, D. M., Troja, E., & Truong, L. M. (2022, March). Teaching effective cybersecurity through escape the classroom paradigm. In *2022 IEEE Global Engineering Education Conference (EDUCON)* (pp. 17-23). IEEE.

Diawati, P., Gadzali, S. S., Abd Aziz, M. K. N., Ausat, A. M. A., & Suherlan, S. (2023). The role of information technology in improving the efficiency and productivity of human resources in the workplace. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *5*(3), 296-302.

Dupuis, M. J. (2017). Cyber security for everyone: An introductory course for non-technical majors. *Journal of Cybersecurity Education, Research and Practice*, *2017*(1), 3.

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE Access*, 10, 52319-52335.

Haney, J. and Lutters, W. G. (2021). Cybersecurity advocates: discovering the characteristics and skills of an emergent role. *Information and Computer Security*, 29(3), 485-499.

Hsiao, S. C. (2021). Effects of the application of virtual reality to experiential education on self-efficacy and learning motivation of social workers. *Frontiers in Psychology*, *12*, 770481.

Ismail, N., Abd Aziz, M. K. N., Arsani, Z., & Harun, M. H. (2021). National Education Philosophy: A Review of Its Application in Malaysia's Education System. *ZAHRA: Research and Tought Elementary School of Islam Journal, 2*(2), 99-111.

Jin, G., Tu, M., Kim, T., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (Edulearn)*, 12(1), 150-158.

Kaicker, A., Mathur, P., Kandula, A., & Kaur, S. (2023). Industry-academia interaction in India: The current scenario and the future. *Journal of Ecophysiology and Occupational Health*, *23*(1), 14-22.

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, 12(10), 417.

Kilhoffer, Z., Zhou, Z., Huang, Y., Kim, P., Yeh, & T., Wang, Y. (2023). "How technical do you get? I'm an English teacher": Teaching and Learning Cybersecurity and AI Ethics in High School. *IEEE Symposium on Security and Privacy (SP)* doi: 10.1109/SP46215.2023.10179333

Kraus, L., Švábenský, V., Horák, M., Matyáš, V., Vykopal, J., & Čeleda, P. (2023). Want to Raise Cybersecurity Awareness? Start with Future IT Professionals. In *Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 1* (pp.236-242).

Langner, G., Skopik, F., Furnell, S., & Quirchmayr, G. (2022). A Tailored Model for Cyber Security Education Utilizing a Cyber Range. In *ICISSP* (pp. 365-377).

Mack, N. A., Mackroy, K., Cook, C., Cummings, R., Pittman, T., & Gosha, K. (2020, March). Evaluating a Cybersecurity Training Program for Non-Computing Major Undergraduate ROTC Students. In *2020 Research on Equity and Sustained Participation in Engineering, Computing, and Technology (RESPECT)* (Vol. 1, pp. 1-2). IEEE.

Maphosa, V. (2024). An overview of cybersecurity in Zimbabwe's financial services sector. F1000Research, 12.

Martin, A., & Collier, J. (2020). Beyond awareness: Reflections on meeting the inter-disciplinary cyber skills demand. In *Cyber Security Education* (pp. 55-73). Routledge.

McDonald, J., Hansen, D., Balzotti, J., Tanner, J., Winters, D., Giboney, J., & Bonsignore, E. (2019). Designing Authentic Cybersecurity Learning Experiences: Lessons from the Cybermatics playable case study. In *Proceedings of the Hawaii International Conference on System Sciences.*

McNulty, M., & Kettani, H. (2020). On cybersecurity education for non-technical learners. In *2020 3rd International Conference on Information and Computer Technologies (ICICT)* (pp. 413-416). IEEE.

Mohd Nawi, N. S., Ramamurthy, L., Shafien, S., Omar, S., & Nik Azim, N. A. F. (2021). Perception of digital reading material for academic purposes among UMK undergraduates. http://myscholar.umk.edu.my/handle/123456789/2737

Mountrouidou, X., Li, X., & Burke, Q. (2018). Cybersecurity in Liberal Arts general education curriculum. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (pp.182-187).

MyCERT. (2023). CyberSecurity Malaysia - Malaysia Computer Emergency Response Team (MyCERT) Incident Statistics. CyberSecurity Malaysia.

Oliveira, L., Chmielewski, A., Rutecka, P., Cicha, K., Rizun, M., Torres, N., & Pinto, P. (2023). Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus - A Case Study of Higher Education Institutions in Portugal and Poland. *IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 168-173). IEEE.

Peker, Y. K., Ray, L., & Da Silva, S (2018). Online cybersecurity awareness modules for college and high school students. *National Cyber Summit* (*NCS)* (pp. 24-33). IEEE.

Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., & Lamberson, C. (2016). Raising cybersecurity awareness among college students. In *Journal of the Colloquium for Information System Security Education* (Vol. 4, No. 1, pp. 17-17).

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the impact of cybersecurity awareness on small and medium enterprises (SMEs) in Wales using intelligent software to combat cybercrime. *Computers*, *11*(12), 174.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173.

Sharevski, F., Trowbridge, A., & Westbrook, J. (2018, March). Novel approach for cybersecurity workforce development: A course in secure design. In *2018 IEEE integrated STEM education conference (ISEC)* (pp. 175-180). IEEE.

Srivatanakul, T., & Annansingh, F. (2022). Incorporating active learning activities to the design and development of an undergraduate software and web security course. *Journal of Computers in Education*, *9*(1), 25-50.

Syarova, S., & Toleva-Stoimenova, S. (2023, June). Cybersecurity Issues in the Secondary and Higher Education Systems' Curricula. In *InSITE 2023: Informing Science+ IT Education Conferences* (p. 003).

Zubir, F., Suryani, I., & Ghazali, N. (2018). Integration of Augmented Reality into College Yearbook. In MATEC Web of Conferences (Vol. 150). EDP Sciences.