International Journal of Research Studies in Education
2026 Volume 15 Number 20, 27-36

A preliminary assessment of cybersecurity OJT experiences, technical competencies and curriculum alignment

Perez-Napalit, Arcely ✉
Holy Angel University, Philippines (anapalit@hau.edu.ph)

ISSN: 2243-7703
Online ISSN: 2243-7711

Received: 4 August 2026 **Revised**: 19 August 2026 **Accepted**: 20 August 2026 OPEN ACCESS
Available Online: 21 August 2026 **DOI**: 10.5861/ijrse.2026.26380

Abstract

The growing demand for cybersecurity professionals highlights the need for academic programs to ensure that graduates possess competencies aligned with industry requirements. This study conducted a preliminary assessment of the On-the-Job Training (OJT) experiences of Cybersecurity graduates by examining their technical competencies, evaluating curriculum alignment with workplace demands, and identifying areas for curriculum enhancement. A descriptive survey was administered to eight graduates who completed their OJT in various organizations. Findings showed that most competency ratings were in the good to excellent range, indicating that the curriculum provided a strong foundation in areas such as ethical hacking, network security, server security, and cloud security. Respondents reported that many of the knowledge and skills acquired from their courses were applied during their internships. However, exposure to advanced industry tools, emerging technologies, artificial intelligence applications, and technical reporting revealed opportunities for further curriculum improvement. Differences in skill utilization were also influenced by the nature of assigned tasks and organizational policies within host companies. The findings suggest that the curriculum is generally aligned with workplace requirements but would benefit from continuous updates to address evolving cybersecurity technologies and industry practices.

Keywords: cybersecurity education, on-the-job training, technical competencies, curriculum enhancement, workforce readiness

A preliminary assessment of cybersecurity OJT experiences, technical competencies and curriculum alignment

1. Introduction

Cybersecurity has become an important concern in education as students and institutions increasingly depend on digital technologies. The need for cybersecurity awareness programs that help students recognize and respond to online risks, particularly those associated with social media, has been emphasized in recent studies (Chahid et al., 2026). Likewise, educating users about cybersecurity practices is essential for protecting personal information and reducing exposure to cyber threats (Shelim, 2024). Educational institutions must also adopt effective and structured cybersecurity education approaches to prepare students for increasingly sophisticated cyberattacks (Salem et al., 2024). Cybersecurity education plays a key role in addressing workforce demands and narrowing the gap between academic preparation and industry requirements. Studies have shown that employers often seek competencies that are not fully developed through existing educational programs (Yusuf, 2024). Other researchers have emphasized the need for curriculum development guided by industry competency requirements and workforce needs (Majanoja & Hakkala, 2023), while curriculum alignment has been identified as essential in preparing graduates for professional cybersecurity roles (Yar et al., 2024).

On-the-Job Training (OJT) complements classroom learning by allowing students to apply their knowledge and skills in actual work environments. Research has shown that OJT enhances learning experiences and prepares students for professional practice through exposure to industry processes and workplace expectations (Loc et al., 2025). Participation in OJT has also been found to improve technical competencies, soft skills, and career readiness (Banes et al., 2025). Furthermore, OJT has been described as a structured learning experience that helps students acquire job-related knowledge and skills (Wangchuk, 2023). Taken together, these studies show that OJT serves as an effective bridge between academic preparation and workplace practice.

In response to the growing demand for cybersecurity professionals, Holy Angel University through its School of Computing offers a Cybersecurity program designed to develop students' technical competencies and professional readiness. As part of the curriculum, students undergo On-the-Job Training (OJT) to gain industry exposure and practical experience. Given the importance of aligning academic preparation with workplace requirements, it is essential to examine how students perceive their technical competencies and the extent to which the curriculum supports the demands encountered during their OJT experiences.

This study aimed to conduct a preliminary assessment of Cybersecurity students' OJT experiences by examining their perceived technical competencies, evaluating curriculum alignment with workplace requirements, and identifying opportunities for curriculum enhancement based on industry exposure and professional practice.

2. Review of Related Literature

Cybersecurity Education and Workforce Preparation - The growing demand for cybersecurity professionals continues to outpace the supply of qualified personnel, highlighting a gap between academic preparation and industry requirements (Dillon & Tan, 2023; Furnell, 2021; Haynes, 2024). This situation has increased the need for educational institutions to review and strengthen their cybersecurity programs to ensure that graduates possess competencies relevant to current workforce demands (Kompara et al., 2026; Murphy et al., 2023). While many programs focus heavily on technical knowledge, employers also expect graduates to demonstrate organizational, communication, and problem-solving skills that support effective cybersecurity practice (Kompara et al., 2026). Efforts to address workforce shortages have led to the expansion of cybersecurity pathways through degree programs, professional certifications, and specialized training initiatives (Ismail et al., 2024). However, developing effective curricula remains a challenge because of the rapidly changing threat landscape and the absence of widely

accepted standards for cybersecurity qualifications (Furnell, 2021; Ismail et al., 2024). Recent studies suggest that stronger collaboration among academic institutions, industry partners, and government agencies, together with experiential learning opportunities and modern instructional technologies, can help improve workforce readiness and better prepare future cybersecurity professionals (Murphy et al., 2023; Ghimire et al., 2024).

Technical Competencies in Cybersecurity - Cybersecurity professionals are expected to possess a combination of technical, professional, and behavioral competencies to perform effectively in different cybersecurity roles. Common competency areas include penetration testing, security operations, digital forensics, incident response, and information security management, highlighting the need for cybersecurity education to remain aligned with workforce requirements (Yamin & Katt, 2019). Beyond technical expertise, employers increasingly value communication, collaboration, adaptability, and problem-solving skills, which are essential for addressing complex and evolving cybersecurity challenges (Schramm et al., 2025; Sumner et al., 2023). Practical learning experiences and hands-on training also play an important role in strengthening students' ability to apply knowledge in real-world situations and respond to workplace demands (Szczepaniuk & Szczepaniuk, 2022). Despite growing interest in cybersecurity education, studies continue to report gaps in students' practical skills and competency development (Módné Takács & Pogátsnik, 2024; Alammari et al., 2022).

Emerging Cybersecurity Technologies and Curriculum Enhancement - Cybersecurity professionals are expected to possess a combination of technical, professional, and behavioral competencies to perform effectively in different cybersecurity roles. Common competency areas include penetration testing, security operations, digital forensics, incident response, and information security management, highlighting the need for cybersecurity education to remain aligned with workforce requirements (Yamin & Katt, 2019). Beyond technical expertise, employers increasingly value communication, collaboration, adaptability, and problem-solving skills, which are essential for addressing complex and evolving cybersecurity challenges (Schramm et al., 2025; Sumner et al., 2023). Practical learning experiences and hands-on training also play an important role in strengthening students' ability to apply knowledge in real-world situations and respond to workplace demands (Szczepaniuk & Szczepaniuk, 2022). Despite growing interest in cybersecurity education, studies continue to report gaps in students' practical skills and competency development (Módné Takács & Pogátsnik, 2024; Alammari et al., 2022).

Curriculum Alignment and Industry Readiness in Cybersecurity Education - Curriculum alignment is essential in ensuring that cybersecurity graduates develop competencies that match current workforce requirements. Effective cybersecurity programs combine theoretical knowledge, hands-on laboratory activities, industry certifications, research opportunities, and competency-based frameworks aligned with recognized standards such as NICE and NIST (Nnadi & Opoku, 2025; Towhidi & Pridmore, 2023). Studies also show that employers expect graduates to possess not only technical expertise but also communication, critical thinking, adaptability, problem-solving, and ethical decision-making skills needed in professional environments (Miranda et al., 2024). To improve workforce readiness, researchers recommend strengthening industry collaboration, practical training, certification opportunities, and experiential learning within cybersecurity programs (Griffin, 2024; Tran et al., 2023). In addition, cybersecurity curricula must continuously adapt to emerging technologies, evolving security practices, and changing industry requirements to ensure graduates remain competitive and prepared for professional roles (Basta et al., 2026). These findings highlight the importance of curriculum innovation and competency-focused program design in enhancing graduate employability and industry readiness.

The reviewed literature highlights the increasing demand for cybersecurity professionals and the need for cybersecurity education programs to align with evolving industry requirements. Effective cybersecurity education requires the development of technical, professional, and behavioral competencies through hands-on learning, industry collaboration, and competency-based curriculum design. Furthermore, emerging technologies continue to influence curriculum development, necessitating continuous program enhancement to ensure graduate preparedness and workforce readiness. Overall, the literature emphasizes the importance of curriculum alignment, practical learning experiences, and continuous improvement in preparing future cybersecurity professionals.

The aim of the study is to assess the OJT experiences of Cybersecurity graduates and examine the alignment of the Cybersecurity curriculum with industry requirements. Specific Objectives

- To describe the OJT experiences of Cybersecurity graduates in terms of their host organizations, assigned roles, and workplace responsibilities.
- To assess the technical competencies of Cybersecurity graduates based on their self-evaluation and experiences during OJT.
- To determine the extent to which technical competencies were utilized during OJT across different workplace settings.
- To examine the alignment between the Cybersecurity curriculum and industry requirements based on the graduates' OJT experiences.
- To identify curriculum strengths, competency gaps, and emerging industry needs encountered during OJT.
- To propose recommendations for curriculum enhancement based on the graduates' feedback and workplace experiences.

3. Methodology

Research Design - This study employed a mixed-methods descriptive design to examine the OJT experiences of Cybersecurity graduates and assess the alignment of the curriculum with workplace requirements. Quantitative data were collected to evaluate graduates' technical competencies, the frequency with which these competencies were used during OJT, and their perceptions of curriculum relevance. Qualitative data, gathered through open-ended responses, were used to gain deeper insights into their workplace experiences, the technologies they encountered, and the challenges they faced. The combination of both approaches provided a more comprehensive view of graduate preparedness and the effectiveness of the curriculum in supporting industry needs.

Researcher Positionality - The researcher is a faculty member of the School of Computing and is familiar with the Cybersecurity curriculum evaluated in this study. To promote objectivity, responses were collected anonymously through an online survey and analyzed based on the information provided by the participants. Standardized data collection and analysis procedures were followed throughout the study to ensure consistency in the interpretation of the findings.

Participants - The participants were graduates from the second graduating cohort of the Cybersecurity program of the School of Computing at Holy Angel University who completed their OJT during Academic Year 2025–2026. During their internship, they were assigned to various organizations, including managed security service providers, financial technology companies, telecommunications firms, educational institutions, and other information technology-related organizations. Their work assignments included technical support, networking, security operations, penetration testing, system administration, and other cybersecurity-related functions. Of the 21 graduates eligible to participate in the study, eight responded to the survey, representing 38.1% of the population.

Instrument - The study utilized a researcher-developed questionnaire designed to gather information on the OJT experiences of Cybersecurity graduates, their technical competencies, and their perceptions of curriculum alignment with industry requirements. The instrument consisted of both closed-ended and open-ended questions and was developed based on the objectives of the study and a review of literature related to cybersecurity education, workforce readiness, technical competencies, OJT experiences, and curriculum alignment (Furnell, 2021; Murphy et al., 2023; Nnadi & Opoku, 2025; Towhidi & Pridmore, 2023).

The questionnaire was organized into five sections. The first section collected information about the respondents and their host organizations. The second section focused on technical competency self-assessment,

where participants rated their competency levels in various cybersecurity and information technology areas using a four-point scale ranging from Fair to Excellent. The third section examined the extent to which technical skills were utilized during OJT, with response options ranging from Daily/Expert to Not Applicable. The fourth section assessed curriculum alignment by examining the relevance of the knowledge, skills, and tools acquired during the program to workplace requirements. The final section consisted of open-ended questions that allowed participants to describe their experiences, identify curriculum strengths and competency gaps, discuss emerging technologies encountered during OJT, and provide recommendations for program improvement.

Data Collection - Data collection was conducted through an online questionnaire administered using Google Forms. The survey link was sent electronically to graduates who had completed their OJT. Prior to participation, the respondents were informed about the purpose of the study and were assured that all information provided would be treated confidentially and used solely for academic research. Participation was voluntary, and respondents were free to complete the questionnaire at their convenience. Responses submitted through the platform were automatically recorded and compiled for subsequent analysis.

Data Analysis - Quantitative responses were first encoded and organized for analysis. Frequency counts and percentages were computed to summarize the respondents' profiles, competency ratings, skill utilization frequencies, and perceptions of curriculum alignment. Weighted means were then calculated to determine the overall level of technical competency.

For the qualitative data, responses to the open-ended questions were reviewed several times to identify recurring ideas and experiences. Similar responses were coded, grouped into categories, and organized into broader themes related to skill application, workplace experiences, curriculum strengths, areas for improvement, and industry expectations. The resulting themes were used to provide additional context and explanation for the quantitative findings.

Trustworthiness of Qualitative Findings - The credibility of the qualitative findings was strengthened through a careful review of the participants' responses. Recurring ideas and experiences were identified and organized into themes that reflected the views of the respondents. Selected participant quotations were used to support the findings and demonstrate how the themes were derived from the data.

Ethical Consideration - Participation in the study was voluntary. Prior to completing the questionnaire, respondents were informed of the objectives of the study and their right to decline participation. Confidentiality and anonymity were maintained throughout the research process, and no personally identifiable information was disclosed in the presentation of results. All information collected was used exclusively for academic and research purposes.

4. Results and Discussion

The respondents completed their OJT in organizations from various sectors, including telecommunications, banking and financial technology (FinTech), outsourcing, education, and managed security service providers (MSSPs). Four respondents were assigned to technical cybersecurity roles such as security operations, penetration testing, and security assessment, while four were assigned to general IT support roles involving helpdesk, networking, and hardware support. This distribution provided exposure to both cybersecurity-specific and general IT environments.

The results indicate that most competency ratings fell within the Good to Excellent categories (33.3 or 75%) as presented in Table 1, suggesting that graduates generally felt adequately prepared to perform technical tasks encountered during OJT. Respondents assigned to cybersecurity-focused organizations, particularly MSSPs and FinTech companies, consistently reported higher competency ratings compared to those assigned to general IT support roles. Participants identified several courses that contributed to their OJT performance, including Ethical Hacking, Network Security, Server Security, Cloud Security, Cybersecurity Policy, and Networking courses. One

participant remarked, "All the technical skills I used during the OJT were covered in my subjects." Another respondent attributed much of their preparedness to the Ethical Hacking course and Cisco-based networking training. These responses suggest that the program provided a strong foundation in the technical areas required during OJT.

Table 1
Technical Competencies of Cybersecurity During OJT

Technical Competency Area	Weighted Mean	Interpretation
Network Security	3.38	Good
Cloud Security	3.25	Good
Defensive Operations	3.38	Good
Server security	3.50	Very Good
Governance and Policy	3.25	Good
System Security	3.25	Good
Overall Mean	**3.33**	**Good**

The frequency of technical skill utilization varied according to the respondents' assigned roles, as shown in Table 2. Most responses fell under the Occasionally category, indicating that many cybersecurity skills were applied only during specific tasks or projects. Students assigned to penetration testing and security assessment roles reported more frequent use of technical skills than those assigned to general IT support functions. Several respondents also reported limited opportunities for hands-on technical work due to organizational policies and restricted access to production systems. As one participant shared, *"Interns are not allowed to touch live systems,"* while another noted that *"My role was strictly administrative."* These findings suggest that the application of technical skills during OJT was influenced largely by the nature of the assigned tasks and the policies of the host organization.

Table 2
Utilization of Technical Skills During OJT

Frequency of Use	Frequency
Daily/Expert	1
Frequently	3
Moderately	8
Occasionally	21
Rarely	4
Not applicable	11
Total	**48**

Participants compared workplace tools and technologies with those encountered in their university laboratories as presented in Table 3. Half of the respondents reported that the technologies used during OJT were similar to those encountered in laboratory activities. However, several respondents noted exposure to more advanced and proprietary technologies. Respondents identified several tools and technologies that were not extensively covered during their coursework, including: Ekahaum, RuckusOne, Burp Suite Professional, Nessus Professional, Wappalyzer, TestSSL.sh, Mobile application testing tools, AI-enabled automation tools, Cloud management platforms and Serverless technologies. One participant stated:"The company used much more advanced and proprietary tools than our labs." Another respondent highlighted the growing use of artificial intelligence, "The use and integration of Artificial Intelligence on automation." These responses suggest that while the curriculum offers a solid foundation, emerging technologies and industry-specific tools continue to evolve faster than academic environments.

Table 3
Curriculum Alignment with Industry Requirements

Curriculum Alignment Observation	Frequency
Same tools/software used in HAU labs	4
More advanced/proprietary tools used by company	3
Older/legacy systems used by company	1
Occasionally	8
Total	**8**

4.1 Curriculum Strengths, Gaps, and Areas for Enhancement

Theme 1: Strong Foundation in Core Cybersecurity Concepts

Several participants reported that courses such as Ethical Hacking, Networking, Cloud Security, and Server Security adequately prepared them for their OJT responsibilities. Mainly 6SERVERSEC, SHSEC, CYBERPOLICY, ETHHACK, and CLOUD and all web-related, network-related, and ethical hacking.

Theme 2: Need for Greater Exposure to Emerging Technologies

Respondents recommended increased coverage of, Artificial intelligence in cybersecurity, Advanced cloud security, Mobile application security testing, Serverless architecture, Advanced networking technologies.

Theme 3: Need for Professional Reporting and Documentation Training

Several participants emphasized that technical reporting was an important skill in industry, areas identified include Vulnerability Assessment Reports, VIS Reports, OWASP Top 10 Mapping, OWASP Testing Guide and CVSS Scoring. Responses stated that "Proper way of creating a report when doing a pen test." And to "Add a dedicated area for reporting. Usage of OWASP Top 10 mapping, OWASP WSTG, and CVSS."

Theme 4: Industry Certifications as a Competitive Advantage

Participants recommended greater support for industry-recognized certifications such as, CompTIA Security+, Ethical Hacking Certifications and NC II Certifications. One respondent stated: "These certifications can be costly yet have become a significant advantage in job applications."

Educational Implications of the Study - The findings of this study provide useful insights for cybersecurity education and curriculum development. For educators, the results highlight the importance of combining theoretical knowledge with practical learning experiences to better prepare students for workplace demands. Although the graduates generally reported good technical competency, their exposure to advanced tools and emerging technologies during OJT suggests the need for continuous curriculum updates and enhanced hands-on training.

For students, the findings underscore the value of building strong foundations in areas such as ethical hacking, network security, and cloud security while also developing skills that respond to emerging industry trends. For academic institutions and curriculum planners, the results demonstrate how OJT experiences can serve as a valuable source of feedback for evaluating curriculum effectiveness. The identified competency gaps and industry requirements may help guide curriculum enhancement, laboratory improvements, industry partnerships, and certification initiatives to better align academic preparation with the needs of cybersecurity.

5. Conclusion and Recommendations

This study examined the OJT experiences of Cybersecurity graduates by assessing their technical competencies, evaluating curriculum alignment with workplace requirements, and identifying areas for improvement. The findings indicate that graduates generally possessed good technical competencies and considered the curriculum relevant to their assigned workplace responsibilities. These results suggest that the program provides a solid foundation in key cybersecurity concepts and skills needed in professional settings. However, the study also identified opportunities for enhancement, particularly in emerging technologies, advanced cybersecurity tools, artificial intelligence applications, cloud security, mobile security testing, and technical reporting.

The findings underscore the importance of continuously reviewing and updating the curriculum to keep pace with evolving industry practices. Greater exposure to industry-standard tools, hands-on laboratory activities, simulations, and project-based learning experiences may further strengthen student preparedness. Additional

training in vulnerability assessment reporting, OWASP methodologies, CVSS scoring, and other professional documentation practices may also help students meet workplace expectations. Strengthening partnerships with industry organizations and certification providers may further enhance learning opportunities and workforce readiness.

Significance of the Findings - The study contributes to ongoing efforts to improve curriculum alignment and workforce readiness in cybersecurity education. By examining graduates' OJT experiences, it provides insight into how academic preparation translates into workplace application and highlights areas where additional support may be needed. The findings may assist educators in refining instructional practices, help students better understand industry expectations, and support academic institutions in making informed decisions regarding curriculum development. More broadly, the study emphasizes the value of continuous curriculum evaluation in preparing graduates for the changing demands of the cybersecurity profession.

Future Work and Limitations - As a preliminary assessment, this study was limited to a small group of graduates and relied on a researcher-developed questionnaire that was not subjected to formal reliability testing or expert validation. Future studies may strengthen the instrument through pilot testing, expert review, and statistical reliability analysis. Further research may involve larger samples, additional graduating cohorts, and feedback from employers, OJT supervisors, and industry partners to provide a more comprehensive evaluation of graduate preparedness and curriculum effectiveness. Comparative studies across institutions may also help identify best practices in cybersecurity education. In addition, future research may examine the impact of curriculum enhancements, industry certifications, and collaborative initiatives on student performance, workplace readiness, and career outcomes.

AI Use Disclosure - Microsoft Copilot (GPT-5 chat model, 2026) was used for language editing and manuscript refinement. All outputs were reviewed and revised by the author, who takes full responsibility for the content of the manuscript. No confidential or personally identifiable data were entered into the AI tool.

6. References

Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Computer Science, 8*, e827. https://doi.org/10.7717/peerj-cs.827

Banes, L., Ochoa, G., Romero, C., Norbe, M. L., & Tolentino, F. (2025). Assessing the impact of on-the-job training program on the academic performance of senior students as a basis to strengthen the OJT implementation for the UDM College of Business Administration curriculum. *APCORE Online Journal, 1*(1), 208-212. https://doi.org/10.65232/8bmjzx93

Basta, S. E., Alkadi, I., & Basta, R. M. (2026). Proposed standards for cybersecurity curricula in higher education. *International Journal of Innovative Science and Research Technology, 11*(3). https://doi.org/10.38124/ijisrt/26mar896

Chahid, A., El Marzak, Y., & Mansouri, K. (2026). Developing a cybersecurity awareness framework to safeguard Moroccan students from social media threats. *Frontiers in Education, 11*, 1719173. https://doi.org/10.3389/feduc.2026.1719173

Dillon, R., & Tan, K.-L. (2023). Cybersecurity workforce landscape, education, and industry growth prospects in Southeast Asia. *Journal of Tropical Futures: Sustainable Business, Governance & Development, 1*(2). https://doi.org/10.1177/27538931231176903

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security, 100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Ghimire, S., Chowdhury, M. A., Tsang, R., Yarnell, R., Heckert, E., Carpenter, J., Lin, Y.-Z., Mamun, M., DeMara, R. F., Rafatirad, S., Satam, P., & Salehi, S. (2024). Interactive framework for cybersecurity education and future workforce development. In *2024 IEEE Frontiers in Education Conference (FIE)* (pp. 1-7). IEEE. https://doi.org/10.1109/FIE61694.2024.10892909

Griffin, A. J. (2024). *Graduates' work readiness? Cyber security curriculum in Australian universities*

[Doctoral dissertation, Edith Cowan University]. https://doi.org/10.25958/3zby-g837

Haynes, G. (2024). *Cyber education and workforce expectations: A quantitative study* [Doctoral dissertation, University of the Cumberlands].

Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Al Bataineh, M., Melhem, S., & Mouheb, D. (2024). Cybersecurity activities for education and curriculum design: A survey. *Computers in Human Behavior Reports, 16*, 100501. https://doi.org/10.1016/j.chbr.2024.100501

Kompara, M., Nemec Zlatolas, L., Turkanović, M., & Hölbl, M. (2026). Importance of cybersecurity competencies in higher education and for employers. *Applied Sciences*, 16(7), 3260. https://doi.org/10.3390/app16073260

Loc, T. B., Ngan, N. T. T., & Luan, N. T. (2025). On-the-job training: Enhance experience and increase success for the student community in Vietnam. *SAGE Open, 15*(1). https://doi.org/10.1177/21582440241311160

Majanoja, A.-M., & Hakkala, A. (2023). Enhancing a cybersecurity curriculum development tool with a competence framework to meet industry needs for cybersecurity. In *Proceedings of the 24th International Conference on Computer Systems and Technologies (CompSysTech '23)* (pp. 123-128). Association for Computing Machinery. https://doi.org/10.1145/3606305.3606325

Miranda, J. P. P., Tayag, M. I., & Canlas, J. D. (2024). Cybersecurity skills in new graduates: A Philippine perspective. *International Journal of Advances in Applied Sciences, 14*(4), 1217-1228. https://doi.org/10.11591/ijaas.v14.i4.pp1217-1228

Módné Takács, J., & Pogátsnik, M. (2024). The presence of cybersecurity competencies in the engineering education of Generation Z. *Acta Polytechnica Hungarica, 21*(6), 107-124. https://doi.org/10.12700/APH.21.6.2024.6.6

Murphy, D., Tryfona, N., & Marshall, A. M. (2023). A targeted study on the match between cybersecurity higher education offerings and workforce needs. *Virginia Journal of Science, 74*(1-2). https://doi.org/10.25778/jx3e-6785

Nnadi, K., & Opoku, J. A. (2025). Cybersecurity curriculum alignment with industry needs: A literature review of educational models integrating labs, certifications, and research. *Sarcouncil Journal of Engineering and Computer Sciences, 4*(12), 64-76. https://doi.org/10.5281/zenodo.17923740

Salem, M., Samara, K., & Al-Tamimi, A.-K. (2024). Navigating challenges in online cybersecurity education: Insights from postgraduate students and prospects for a standardized framework. *ACM Transactions on Computing Education, 24*(4), Article 56. https://doi.org/10.1145/3703163

Schramm, L. T., Lin, R., & Wei, H.-L. (2025). Beyond technical training: A cybersecurity skills framework for non-professionals. In *Proceedings of the 2025 Computers and People Research Conference (SIGMIS-CPR '25)* (Article 14, pp. 1-8). Association for Computing Machinery. https://doi.org/10.1145/3716489.3728444

Shelim, R. (2024). Cybersecurity in education [Master's thesis, Montclair State University]. Montclair State University Digital Commons. https://digitalcommons.montclair.edu/etd/1441/

Sumner, M., Pearlson, K., Mazzola, D., & Maurer, C. (2023). What technical and professional skills are needed for cybersecurity roles? *WISP 2023 Proceedings*, Article 5. https://aisel.aisnet.org/wisp2023/5

Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy, 46*(3), 102282. https://doi.org/10.1016/j.telpol.2021.102282

Towhidi, G., & Pridmore, J. (2023). Aligning cybersecurity in higher education with industry needs. *Journal of Information Systems Education, 34*(1), 70-83.

Tran, B., Benson, K. C., & Jonassen, L. (2023). Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce. *Journal of Cybersecurity Education, Research and Practice, 2023*(2), Article 2. https://doi.org/10.32727/8.2023.19

Wangchuk, P. (2023). Examining the influence of on-job training (OJT) on student learning: A study focusing on the 6th cohort of the Diploma in Materials and Procurement Management Program at Jigme Namgyel Engineering College in Dewathang. *Journal of Applied Engineering, Technology and Management,*

3(1), 23-31. https://doi.org/10.54417/jaetm.v3i1.100

Yamin, M. M., & Katt, B. (2019). Cyber security skill set analysis for common curricula development. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19)* (Article 37, pp. 1-8). Association for Computing Machinery. https://doi.org/10.1145/3339252.3340527

Yar, M. A., Goh, H. G., Adnan, K., Gan, M. L., & Ponnusamy, V. (2024). Bridging cybersecurity education and industry demands: Mapping and prioritizing curriculum guidelines. In *2024 International Conference on Future Technologies for Smart Society (ICFTSS)* (pp. 188-193). IEEE. https://doi.org/10.1109/ICFTSS61109.2024.10690269

Yusuf, O. I. (2024). Bridging the gap: Aligning cybersecurity education with industry needs. *International Journal of Information Technology & Computer Engineering, 4*(3), 1-8. https://doi.org/10.55529/ijitc.43.1.8