

THE ROLE OF HIGHER EDUCATION IN PREPARING FOR AND PREVENTING CYBER-ATTACKS

Amal Mersni, Nedžla Šehović, Nejira Subašić, Nur Rustempašić



Background & Overview

Cyber-attacks are rising as digital reliance grows. Key challenges in cybersecurity education include:

- Cybersecurity workforce gap of 3.5 million [1]
- Universities must train specialists and promote cross-disciplinary awareness
- Limited data on non-IT student access to cyber programs [2]

This review examines how cybersecurity education is structured, delivered, and accessible to non-IT students.

Methodology

We conducted a qualitative systematic literature review, guided by the **PRISMA framework**. Figure 1 outlines the study selection and **thematic analysis process** used to answer our research questions.

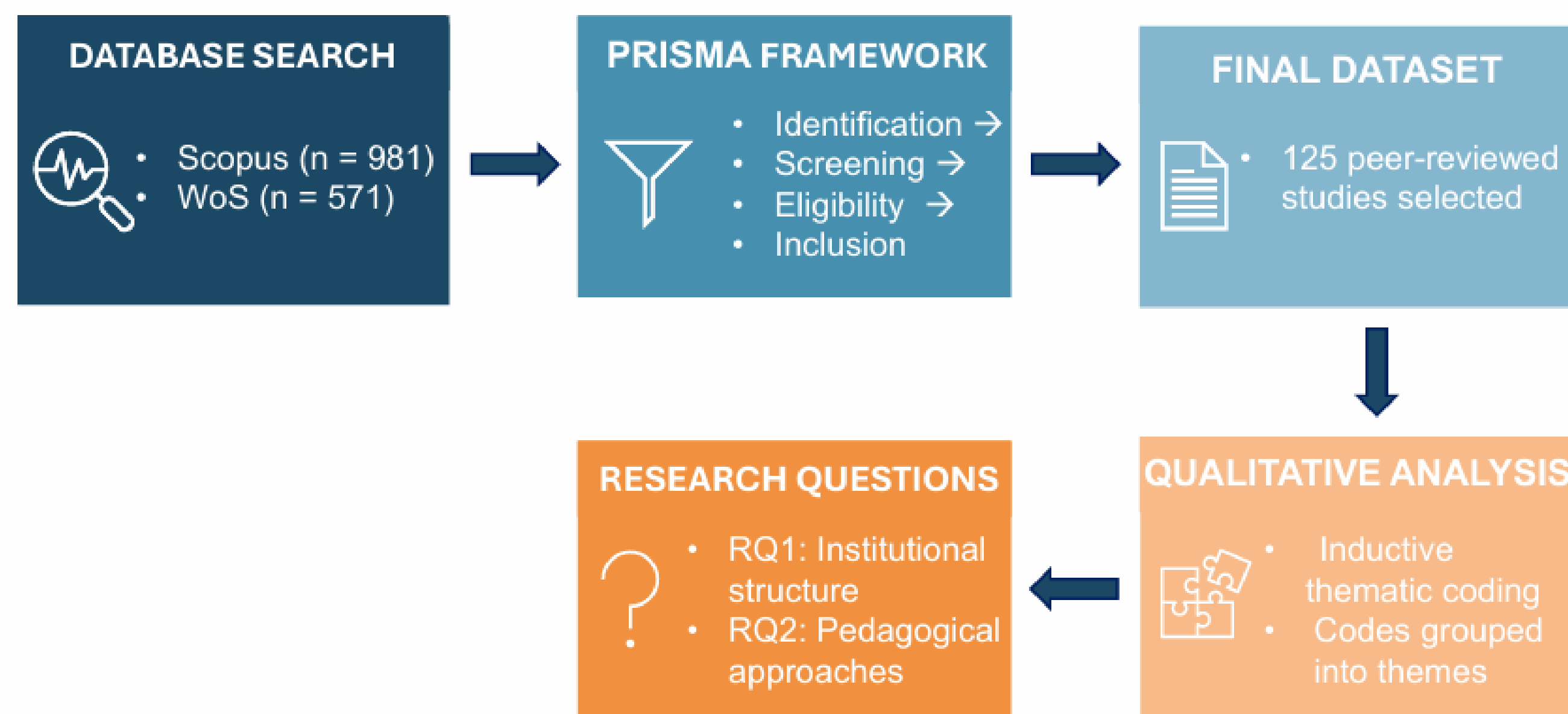


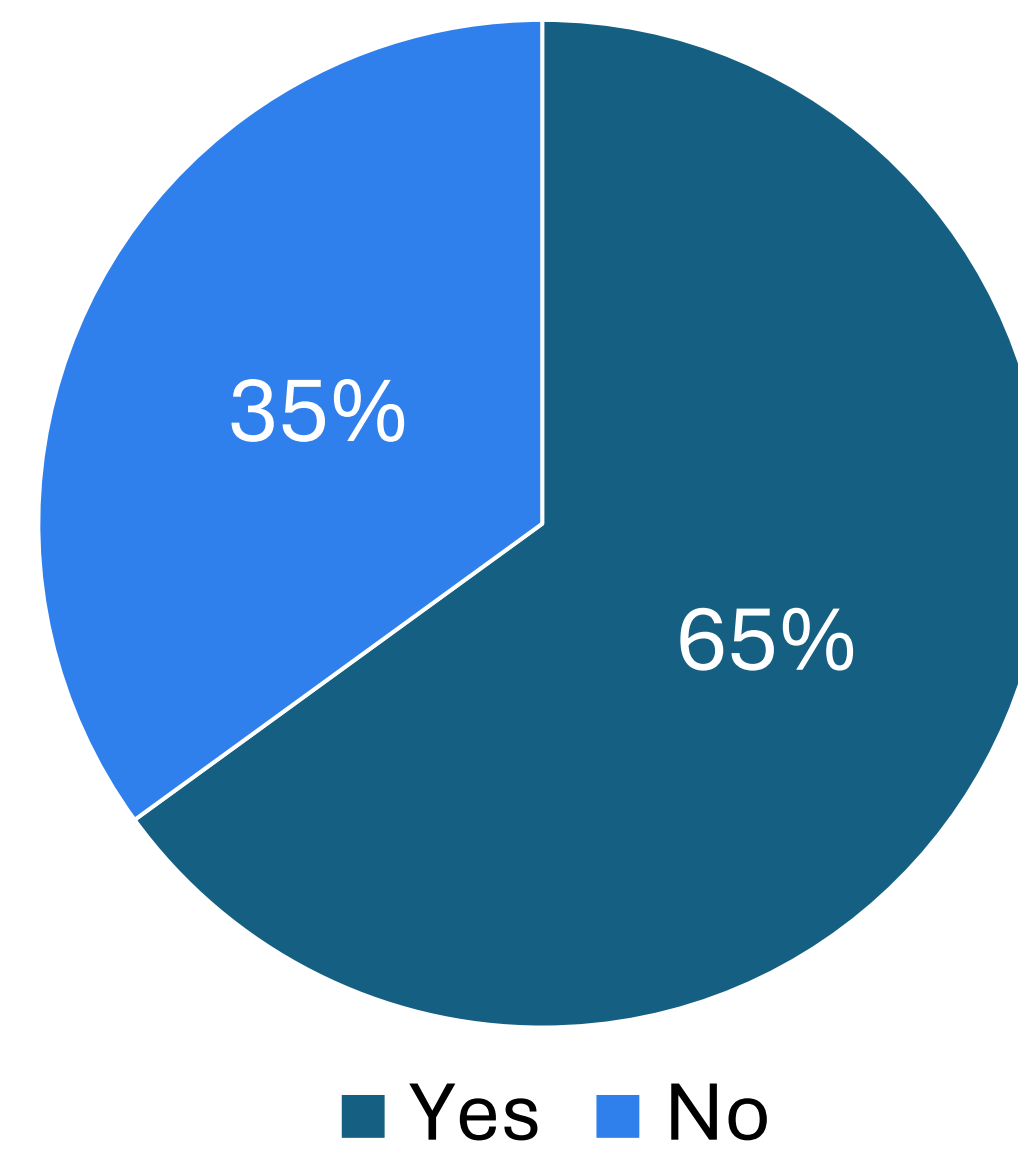
Figure 1. Systematic Review Workflow Using PRISMA and Thematic Analysis

This process ensured a transparent study selection and directly informed the themes linked to **RQ1 and RQ2**.

Key Findings

Our review reveals that **cybersecurity education remains narrowly focused on technical fields**, limiting wider participation. This is especially troubling given external data showing that **65% of organizations faced a cyberattack**, yet only **27% were prepared** (Figure 2).

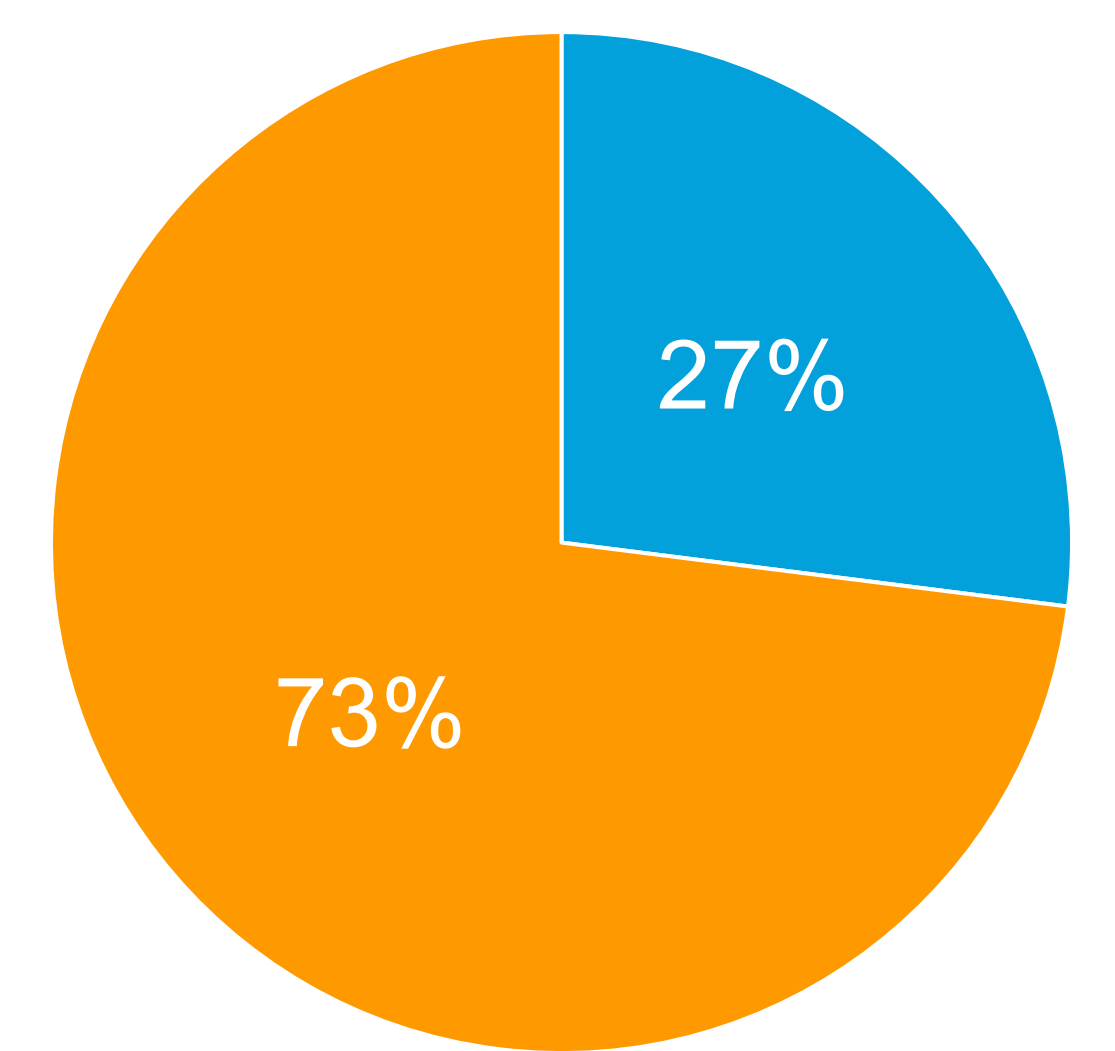
Experienced a Cyberattack?



■ Yes ■ No

Source: [3]

Were they prepared?



■ Prepared ■ Unprepared

Source: [3]

Figure 2. Cyberattack Incidence and Organizational Preparedness

As shown in the Figure 3, while active learning methods dominate (**63.6%**), inclusive teaching strategies are rare, reducing access for **non-technical students**.

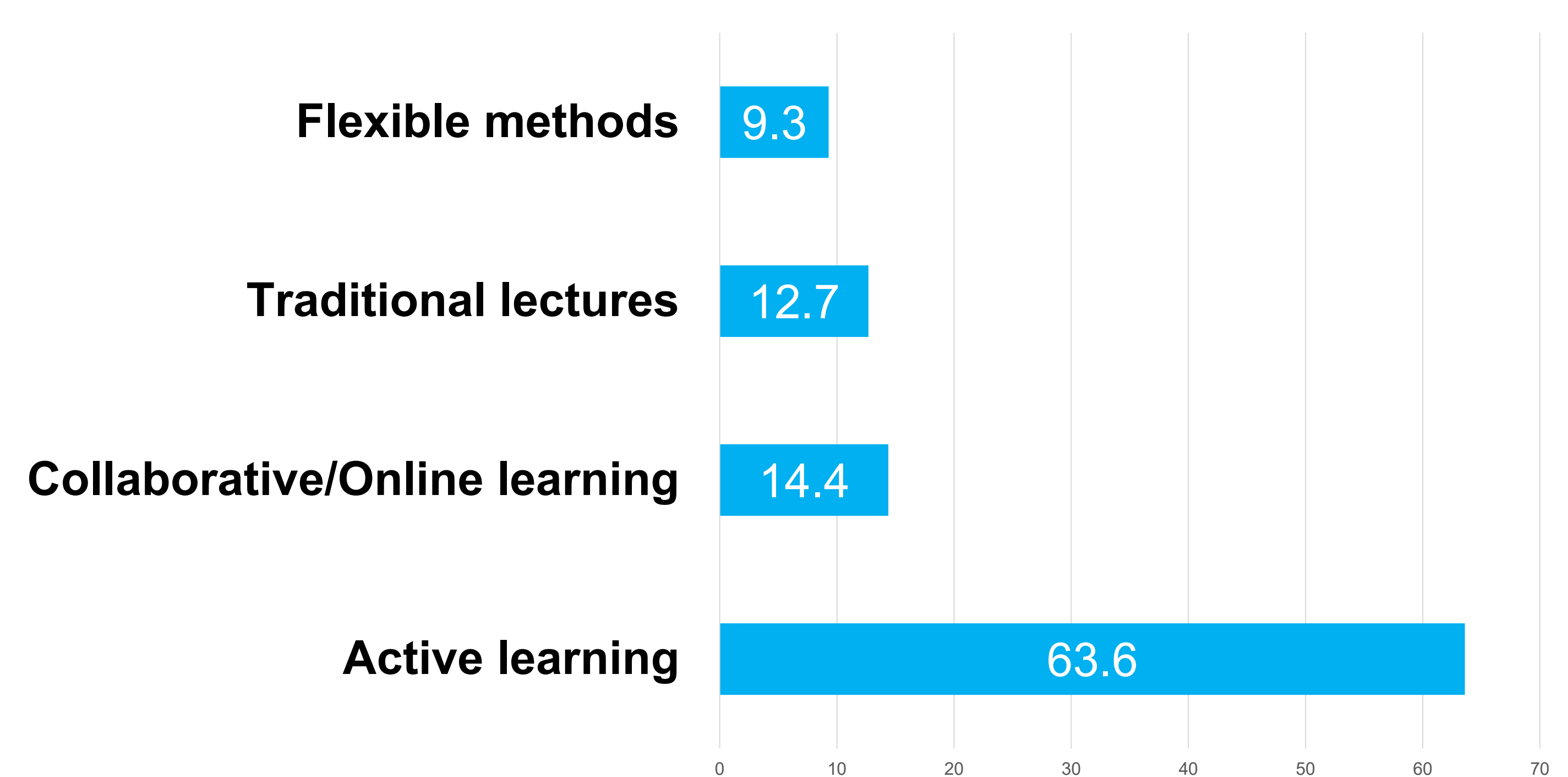


Figure 3. Distribution of Teaching Approaches in Cybersecurity Education

Conclusions

Universities must broaden their cybersecurity mission by:

- Offer **joint courses across faculties** (e.g., CS, Business, Law) to mirror real-world cybersecurity.
- Provide **practical, scenario-based modules** that any student can take, regardless of major.
- Ensure course listings clearly state the target audience, department, and teaching method [4, 5].

By addressing these points, universities can simultaneously **widen participation** and mirror the **interdisciplinary realities** of modern cybersecurity practice.

References

- [1] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respicio, "Cybersecurity education: Evolution of the discipline and analysis of master programs," *Computers & Security*, vol. 75, pp. 24–35, Jun. 2018, doi: <https://doi.org/10.1016/j.cose.2018.01.015>.
- [2] E. Kim and R. Beuran, "On designing a cybersecurity educational program for higher education," *Proceedings of the 10th International Conference on Education Technology and Computers - ICETC '18*, 2018, doi: <https://doi.org/10.1145/3290511.3290524>.
- [3] Varonis, "31 Must-Know Education Cybersecurity Statistics," *Varonis Blog*, Mar. 7, 2024. [Online]. Available: <https://www.varonis.com/blog/education-cybersecurity-statistics>
- [4] Rūta Pirta-Dreimane et al., "Application of intervention mapping in cybersecurity education design," *Frontiers in Education*, vol. 7, Nov. 2022, doi: <https://doi.org/10.3389/educ.2022.998335>.
- [5] N. Swain, "A Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum (CSETA)," 2014 ASEE Annual Conference & Exposition Proceedings, doi: <https://doi.org/10.18260/1-2--19964>.



12th ACM Celebration of Women in Computing: womENCourage™
Braşov, Romania
17-19 September, 2025
Theme: Computer Science: a Catalyst for Educational Change

