

Interdisciplinary Cybersecurity Education: A Systematic Review of Institutional and Pedagogical Practices

Amal Mersni
Faculty of Engineering and
Natural Sciences
International University of
Sarajevo
Sarajevo, Bosnia and
Herzegovina
amersni@ius.edu.ba

Nur Rustempašić
Faculty of Engineering and
Natural Sciences
International University of
Sarajevo
Sarajevo, Bosnia and
Herzegovina
nrustempašić@student.ius.edu.ba

Nejira Subašić
Faculty of Engineering and
Natural Sciences
International University of
Sarajevo
Sarajevo, Bosnia and
Herzegovina
nsubasic@student.ius.edu.ba

Nedžla Šehović
Faculty of Engineering and
Natural Sciences
International University of
Sarajevo
Sarajevo, Bosnia and
Herzegovina
nsehovic@student.ius.edu.ba

ABSTRACT

Cybersecurity education directly impacts our ability to mitigate increasingly frequent and sophisticated cyber threats. Universities have a critical responsibility not only to train cybersecurity professionals but also to educate all students about cyber risks, regardless of their major. Despite an increase in cybersecurity programs, there is limited understanding of how these programs are structured, especially their availability and effectiveness for students outside technical fields. This qualitative systematic review, guided by the PRISMA framework and employing inductive thematic analysis, examines literature from Web of Science and Scopus (2012–2025). Findings reveal significant variation in program structure, predominantly confined within technical disciplines, and limited use of inclusive pedagogical methods. To address this gap, we propose universities adopt interdisciplinary curricula and inclusive pedagogies, enhancing cybersecurity awareness and skills beyond traditional tech disciplines.

CCS CONCEPTS

• Security and privacy → Human and societal aspects of security and privacy • Social and professional topics → Professional topics → Computing education

KEYWORDS

Cybersecurity education, Interdisciplinary learning, Pedagogical methods, Higher Education, Systematic Literature Review, PRISMA

1 Introduction

Cyber-attacks are growing more frequent and sophisticated as our dependence on digital systems deepens. Safeguarding critical services is now a national and global priority, yet the 2023 (ISC)² Workforce Report notes a shortfall of roughly 3.5 million cybersecurity professionals [1]. Universities are in an excellent position to educate future specialists by providing formal cybersecurity training and raising cyber-awareness across disciplines. Although degree programs in cybersecurity are multiplying, the current literature provides limited insight into their

structure and how accessible they are to students outside of traditional technical disciplines. Universities increasingly teach cybersecurity, yet the formats of these programs vary widely, particularly concerning accessibility for non-IT students [2]. Therefore, we need clearer insight into how institutions can open cybersecurity courses to a broader mix of majors and integrate cybersecurity topics into non-technical studies effectively [3]. Despite the expansion of cybersecurity programs, few studies have thoroughly examined their interdisciplinarity or pedagogical design. Little detailed evidence exists on pedagogical methods, their suitability for non-technical students, and how effectively they equip students with competencies to respond to real cybersecurity threats [4]. This research bridges this gap by examining how cybersecurity education is positioned within universities, cataloguing pedagogical approaches, and assessing how effectively these approaches prepare students beyond traditional tech disciplines. Specifically, the study is guided by the following research questions:

RQ1: How is cybersecurity education positioned within university structures, and to what extent is it confined to technical disciplines?

RQ2: What pedagogical approaches do universities adopt in cybersecurity education, and to what extent do these approaches support interdisciplinary participation and inclusivity for non-technical students?

2 Methodology

This study employs a qualitative systematic literature review guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. To address the research questions, we applied inductive thematic analysis, which allowed us to identify themes directly from the content of selected studies without relying on pre-defined categories. We assigned codes to elements like teaching departments, course accessibility, instructional models, and inclusion mechanisms. These codes were then grouped into broader themes aligning with study objectives. The PRISMA framework ensured a clear and repeatable study selection process. The four PRISMA stages—identification, screening, eligibility, and inclusion—were used only to select and document studies, not for the analysis itself.

As shown in the PRISMA flow diagram (Figure 1), we initially identified 1,552 records from two databases: Scopus (n = 981) and Web of Science (n = 571). Scopus and Web of Science were explicitly selected as databases due to their extensive coverage of peer-reviewed scholarly literature, recognized quality standards, and comprehensive indexing of multidisciplinary research. Using these two databases explicitly ensured rigorous and representative sampling of current research literature on cybersecurity education.

After removing 102 duplicates, 1,450 records were screened. From these, 321 reports were selected for full-text review, resulting in a final corpus of 125 peer-reviewed studies published between 2012 and 2025. All coding was performed manually in Excel. After first-cycle coding, we conducted second-cycle thematic grouping, yielding four overarching themes for each research question.

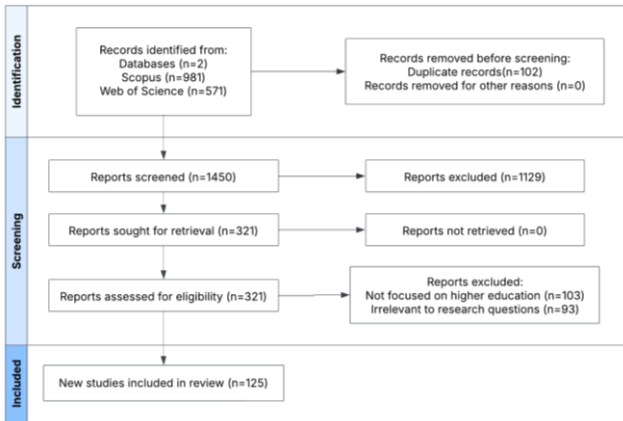


Figure 1: PRISMA flowchart

2 Data Analysis and Results

An analysis of 125 peer-reviewed articles revealed clear trends within the structuring and delivery of cybersecurity education by universities. The inductive thematic analysis identified four key institutional positioning themes based explicitly on indicators of institutional contexts and accessibility.

Table 1: Thematic Analysis Table

Theme	Code	% of studies
Technical disciplinary siloing	“computer science”, “engineering”, “mandatory for CS”, “CS-only”	57.6%
Limited interdisciplinary reach	single-dept elective, no, non-CS-enrolment allowed	14.4%
Emerging cross-faculty models	interdisciplinary team-taught, open elective, business/law	12.0%
Institutional ambiguity	department stated, audience unclear, MOOC/external	16.0%

The results shown in Table 1 explicitly indicate that most cybersecurity education programs (72 studies, 57.6%) remain primarily within technical fields such as computer science and engineering departments, clearly illustrated by direct quotes from analyzed studies, such as: "Course is required for all CS juniors; taught solely in the School of Engineering." Combined with 18 studies (14.4%) offering electives explicitly restricted to technical majors, exemplified by statements such as "Elective open to CS, IT, and IS majors; prerequisites include network security," nearly three-quarters of cybersecurity education remains inaccessible to non-technical students. Only 12% of studies demonstrated interdisciplinary models developed across multiple faculties, illustrated by initiatives described as "Co-developed by Computer Science & Law, open to all second-year students," suggesting substantial room for institutional improvement toward inclusivity and interdisciplinarity. Institutional ambiguity (16%) explicitly refers to unclear or unspecified institutional contexts, including studies that report cybersecurity courses or workshops without clearly identifying departments, target audiences, or explicitly mentioning external MOOC platforms.

The inductive thematic analysis further identified five distinct pedagogical themes. Most studies (n=35, 63.6%) employed *active and experiential learning methods* characterized explicitly by practical engagement such as project-based, game-based, and simulation-based approaches. *Collaborative and social learning* appeared explicitly in seven studies (12.7%), promoting peer interactions suitable for mixed-discipline student groups. *Digital and remote flexibility methods* (n=6, 10.9%), including e-learning and virtual learning, explicitly offered potential to engage non-traditional or part-time students. *Traditional lecture-based methods* (n=4, 7.3%) explicitly emerged as barriers to inclusivity due to passive delivery and technical jargon, reducing accessibility for non-technical learners. Lastly, limited pedagogical innovation (n=3, 5.5%), which included adaptive and awareness-based learning, was least common, explicitly suggesting significant untapped potential for inclusive and innovative pedagogical strategies.

Overall, the thematic analysis explicitly answers the research questions: cybersecurity education remains predominantly confined to technical disciplines (RQ1), and pedagogical approaches explicitly supporting inclusive, interdisciplinary participation remain underdeveloped (RQ2). Structural institutional siloing and passive pedagogical methods explicitly identified as barriers significantly limit interdisciplinary engagement, despite promising examples of emerging cross-faculty models and innovative pedagogies.

4 Conclusions and Recommendations

Universities ought to respond to a broader educational mission in cybersecurity by first acknowledging that, while cybersecurity is fundamentally technical and requires robust technical training, interdisciplinary collaboration can greatly enrich students'

educational experiences. Encouraging explicitly designed interdisciplinary cybersecurity curricula across faculties can reflect the field's complex realities without sacrificing technical rigor. Equally important, universities should actively broaden participation by explicitly employing diverse, inclusive pedagogical methods such as gamification and scenario-based learning, especially for students from non-technical backgrounds. Finally, enhancing transparency through explicit and standardized reporting practices, clearly identifying target audiences, departmental affiliations, and teaching methods, would significantly support comparative research, program replication, and continuous improvement. By explicitly addressing these recommendations, universities can widen participation, enhance interdisciplinary education, and better align their programs with the evolving, multidisciplinary demands 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] 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/feduc.2022.998335>.
- [4] 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>.