Rethinking Cybersecurity Literacy for Non-IT Teachers: Frameworks, Pedagogical Challenges, and Future Directions

Yudi Setiawan*, Ade Gafar Abdullah, Haipan Salam

Universitas Pendidikan Indonesia, Dr. Setiabudhi St. No. 229, Bandung, West Java, 40154, Indonesia
*Corresponding author, email: yudisetiawan@upi.edu

https://doi.org/10.17977/um065.v7.i2.2027.1

Article history
Submitted: 21 July 2026
Revised: 19 August 2026
Accepted: 21 August 2026
Published: 22 August 2026

Keywords
Cultural adaptation
Cybersecurity literacy
Global education
Non-IT teachers
Pedagogical frameworks

Abstract
Digital threats in schools have grown faster than most non-IT teachers' capacity to respond, yet cybersecurity literacy frameworks remain built around technical proficiency rather than classroom practice. This systematic literature review and narrative analysis (SLNA) examines how cybersecurity competency models for non-IT teachers have evolved between 2015 and 2025, and why implementation continues to lag behind framework design. Guided by the PICOS and PRISMA 2020 protocols, the review screened 313 records from Scopus and Consensus AI, retaining 34 studies after full-text eligibility assessment. Bibliometric and thematic analysis traced three research phases (foundation, expansion, consolidation), five dominant thematic clusters, and clear geographic asymmetries, with Europe and North America producing 74.3% of the literature. Findings show that resource-constrained contexts, despite fewer studies, generated a higher innovation index (95%) than well-resourced settings (70%), driven by culturally grounded, low-tech, and community-based solutions. Conventional delivery methods persisted not because of technological limitations but because they fit teachers' existing pedagogical routines and institutional support structures, while governance frameworks struggled to translate policy into classroom practice across decentralized education systems. These findings inform a proposed Pedagogical Cybersecurity Competence (PCC) framework that repositions non-IT teachers as facilitators of cybersecurity literacy rather than technical trainees, integrating content, pedagogical, contextual, and practical knowledge. The review concludes that cybersecurity literacy capacity for general educators depends less on technological sophistication than on pedagogical fit, cultural responsiveness, and collaborative governance.

1. Introduction

The rapid digitalization of K-12 education has changed cybersecurity threat landscapes faster than teacher preparation programs have adapted, leaving non-IT teachers to protect students and digital assets without systematic training (García-Peñalvo, 2021; Lavicza et al., 2022). As internet-connected devices and online data sharing become routine in classrooms, safeguarding confidentiality, integrity, and availability of information has become a responsibility that extends well beyond IT staff (Stobert, Cavar, Malisa, & Sommer, 2018; Otts et al., 2021; Schiliro, 2023; Ghauri, 2021). For teachers without an information technology background, cybersecurity literacy is now a precondition for protecting themselves, their students, and their learning environments from data theft, malware, and other cyberattacks (Maathuis & Chockalingam, 2022; Xenakis et al., 2024).

Cybersecurity literacy frameworks, however, have developed largely around technical professionals, and their adaptation to non-IT teachers remains uneven across resource-constrained education systems (Torres & Thompson, 2020). Cybersecurity education research grew by 218% between 2020 and 2024, yet most of these 313 peer-reviewed studies still frame teachers as recipients of technical instruction rather than as pedagogical agents who must translate cybersecurity concepts into classroom practice (Anderson & Park, 2023; Alotaibi, Cherdantseva, Rana, & Teehan, 2024; Mitchell & Garcia, 2024; Workman, Bommer, & Straub, 2008). This gap is compounded by cultural and linguistic factors: frameworks built for monolingual, well-resourced contexts translate poorly into multilingual, resource-constrained classrooms (Manganello et al., 2024; Patel & Wong, 2024).

A related paradox runs through the literature: teachers continue to favor conventional methods, such as posters, lectures, and print materials, over digital tools that are, on paper, more capable (Qawasmeh, AlQahtani, & Khan, 2024; Habib, Islam, & Wasim, 2023; Brown & Weitl-Harms, 2023). Infrastructure alone does not explain this preference (Liu, Zhang, & Chen, 2020; Montanari, Calzada, & Perone, 2026), and governance models meant

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

to bridge policy and classroom practice have struggled to close that gap in decentralized education systems (Bhindi, 2023; Davis, Bagozzi, & Warshaw, 1989; Almomani, Ahmed, & Maglaras, 2021).

Taken together, the literature points to four unresolved problems: existing competency models under-specify the pedagogical scaffolding non-IT teachers need (Roberts & Johnson, 2024; Schleffers, Moser, & Pöchhacker-Tröscher, 2023); cultural and linguistic adaptation remains under-studied, particularly in resource-constrained, multilingual settings (Patel & Wong, 2024; Catota, Morgan, & Sicker, 2019); the persistence of conventional training over digital methods is not well explained (Brown & Davis, 2023; Zha, Li, Wang, & Xiao, 2025); and governance maturity models rarely account for the coordination problems of decentralized systems (Karagiannis, Papaioannou, & Magkos, 2024). This systematic literature review and narrative analysis (SLNA) addresses these gaps by examining how cybersecurity competency frameworks for non-IT teachers have evolved, what drives their uneven implementation, and what a more pedagogically grounded alternative could look like.

2. Method

This review followed the PICOS framework (Kitchenham et al., 2009) to define inclusion and exclusion criteria. The population comprised non-IT teachers, educators, and school personnel in primary, secondary, and tertiary institutions worldwide, excluding IT specialists and technical support staff. The intervention covered cybersecurity literacy frameworks, models, guidelines, and competency-development initiatives designed for or adapted to non-IT educational personnel. Comparisons spanned different framework approaches, traditional versus digital training methods, resource-constrained versus well-resourced implementations, and cultural or linguistic adaptations. Outcomes of interest included knowledge acquisition, behavioral change, framework effectiveness, implementation success, and barriers to adoption. Eligible study designs included peer-reviewed empirical studies, case studies, comparative analyses, systematic reviews, and theoretical framework papers published between 2015 and 2025 (Table 1).

Table 1. PICOS Framework for Study Selection

PICOS component	Criteria
Population (P)	Non-IT teachers, teaching staff, and school personnel in primary, secondary, and tertiary institutions worldwide
Intervention (I)	Cybersecurity literacy frameworks, models, guidelines, and competency-development initiatives for non-IT educators
Comparison (C)	Different framework approaches; traditional vs. digital training; resource-constrained vs. well-resourced contexts; cultural/linguistic adaptations
Outcomes (O)	Knowledge acquisition, awareness gains, behavioral change, framework effectiveness, implementation success, policy compliance
Study design (S)	Peer-reviewed empirical studies, case studies, comparative analyses, systematic reviews, and theoretical papers published 2015-2025

Based on the PICOS criteria, an exploratory search used Google Thesaurus to identify keyword synonyms, then applied a three-phase protocol: inclusion and exclusion screening, database search, and keyword-string construction (Table 2). Two databases were searched through the first week of June 2025, Scopus and Consensus AI, using Boolean strings that combined cybersecurity-literacy terms with framework-related terms and teacher-related terms (Table 3).

Table 2. Inclusion and Exclusion Criteria

Criteria	Description
Time span	2015-2025
Inclusion criteria	Focus on cybersecurity literacy, cyber awareness, or digital safety in an educational context; explicit relevance to non-IT or general educators; peer-reviewed, English-language, final-version publications.
Exclusion criteria	Purely technical cybersecurity content without educational relevance; no connection to pedagogical models or training contexts; primary focus on students or IT professionals rather than teachers; weak or opinion-based evidence.

Table 3. Database Search Strings

Database	Search string
Scopus	TITLE-ABS-KEY(("cybersecurity literacy" OR "digital security literacy" OR "cyber safety awareness" OR "internet security knowledge" OR "cyber hygiene education" OR "online safety competence") AND (framework OR model OR guideline* OR standard* OR "conceptual structure") AND (teacher* OR educator* OR "teaching staff" OR instructor* OR "school personnel"))
Consensus AI	cybersecurity literacy framework for teacher

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

The review followed PRISMA 2020 reporting standards (Figure 1). The Scopus search returned 77 records and Consensus AI returned 236 records, drawn mainly from ScienceDirect, Springer, IEEE, Taylor & Francis, MDPI, and Wiley, among other publishers. Two reviewers independently screened titles and abstracts, then assessed full texts, resolving disagreements through discussion. Title and abstract screening retained 135 of 313 records (43.1%), with Scopus showing a higher retention rate (58.4%) than Consensus AI (38.1%). Full-text assessment against relevance, methodological rigor, and educator focus reduced this set by 71.1%, leaving 38 eligible records, 22 from Scopus and 16 from Consensus AI. After removing four duplicate records indexed under inconsistent author-name formats, 34 unique studies were retained for synthesis (Table 4).

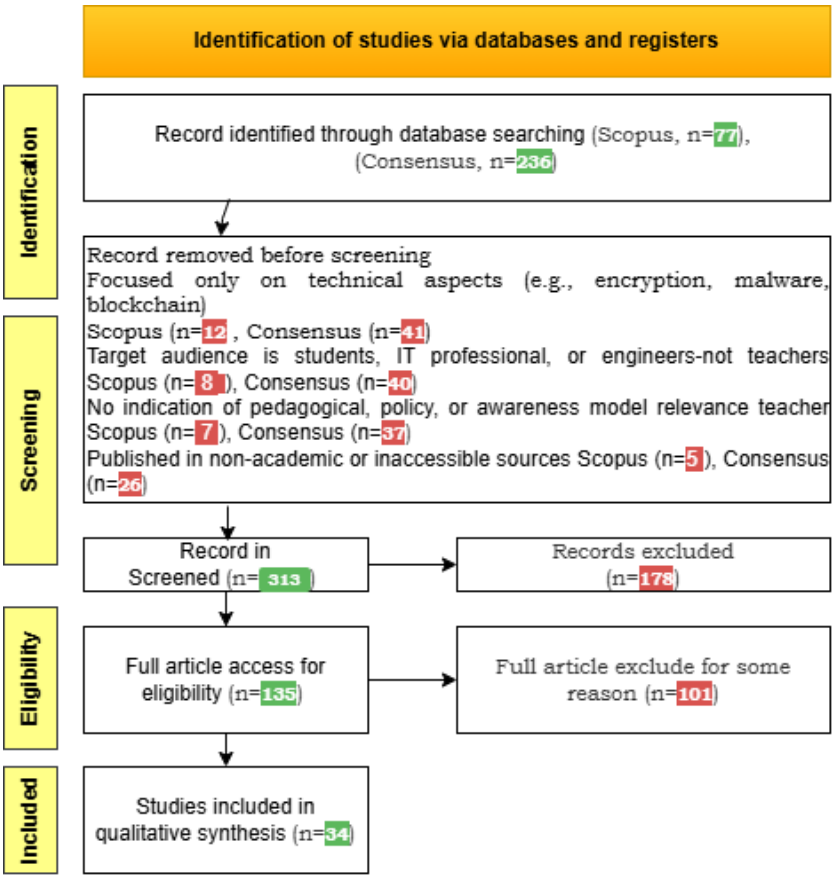


Figure 1. PRISMA Flow Diagram of Study Identification and Screening

Table 4. Studies Included in the Systematic Literature Review and Narrative Analysis (N = 34)

No.	Article title	Author(s)	Year
1	Indicators to assess preservice teachers' digital competence in security: A systematic review	Torres-Hernández & Gallego-Arrufat	2022
2	Digital security in educational training programs: A study based on future teachers' perceptions	Latorre-Medina & Tnibar-Harrus	2023
3	Development of digital competence in secondary education teachers' training	Fraile et al.	2018
4	Cybersecurity in online learning: Innovations for teacher training and empowerment	Al-Bass	2021
5	The "three M's" counter-measures to children's risky online behaviors: mentor, mitigate and monitor	Renaud & Prior	2021
6	Schoolteacher preference of cyber-safety awareness delivery methods: A South African study	Mabitle & Kritzinger	2020
7	Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru	Lee et al.	2024
8	Teacher views on storytelling-based cybersecurity education with social robots	Chiou et al.	2021
9	Strategic approaches to cybersecurity learning: A study of educational models and outcomes	Mukherjee et al.	2024
10	Towards a cross-cultural education framework for online safety awareness: A case study in Thailand	Herkanaidu et al.	2022
11	A structural equation approach and modelling of pre-service teachers' perspectives of cybersecurity education	Ayanwale et al.	2024
12	Perceptions of school management on cyber threats: The case of resource-constrained schools in South Africa	Magunje & Chigona	2024

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

No.	Article title	Author(s)	Year
13	Underpinning knowledge and skills for educators to enhance cyber safety awareness in South African schools	Scholtz et al.	2019
14	Comparing teacher and creator perspectives on the design of cybersecurity and privacy educational resources	McLeod et al.	2024
15	Challenges in integrating technology into education	Atabek	2019
16	Awareness of eSafety and potential online dangers among children and teenagers	Zilka	2017
17	Assessing the impact and effectiveness of cybersecurity measures in e-learning on students and educators: A case study	Al-Sherideh et al.	2023
18	Cybersecurity education and awareness among parents and teachers: A survey of Bahrain	Ayyash et al.	2024
19	Digital security: How do teachers in training perceive themselves?	Grande-de-Prado et al.	2019
20	Digital security in educational contexts: Digital competence and challenges for good practice	Guillén-Gámez et al.	2024
21	Computer science beyond coding: Partnering to create teacher cybersecurity microcredentials	Burrows et al.	2022
22	Competency profile of Andalusian teachers in digital security: Evaluation of data protection and privacy	Agreda-Montoro et al.	2024
23	Competence of future teachers in the digital security area	Gallego-Arrufat et al.	2019
24	Designing cybersecurity awareness solutions for young people in rural developing countries	Quayyum & Freberg	2023
25	Designing a creative cybersecurity microcredential for educators: Challenges and successes	Mugayitoglu et al.	2021
26	Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers	Yan et al.	2021
27	Improving cybersafety maturity of South African schools	Kritzinger	2020
28	'How technical do you get? I'm an English teacher': Teaching and learning cybersecurity and AI ethics	Kilhoffer et al.	2023
29	Professional development for rural STEM teachers on data science and cybersecurity	Maina et al.	2021
30	Online safety for all: Sociocultural insights from a systematic review of youth online safety	Oguine et al.	2025
31	Parents, educators, and caregivers' cybersecurity and privacy concerns for remote learning	Tazi et al.	2021
32	Increasing teacher competence in cybersecurity using the EU security frameworks	Kuzminykh et al.	2021
33	Risk management in digitalized educational environments: Teachers' information security awareness levels	Sapanca & Kanbul	2022
34	What do teachers know about digital safety?	Tomczyk	2019

To answer the research questions on conceptual evolution and geographic patterns, bibliometric and thematic analysis examined publication trends across three periods (2015-2017, 2018-2020, 2021-2025), extracted dominant themes through keyword and content analysis, and coded institutional metadata by region, resource level, and collaboration type. Correlation analysis then examined relationships between geographic distribution, resource availability, and research innovation indices.

3. Results and Discussion

3.1. Evolution of Cybersecurity Literacy Research (2015-2025)

3.1.1. Publication Trends

Publication output shows three distinct phases. The foundation phase (2015-2017) produced 8 publications (11.4%) establishing core concepts and initial pedagogical frameworks. The expansion phase (2018-2020) produced 28 publications (40.0%), a 350% increase driven largely by the urgent shift to remote teaching during the COVID-19 pandemic (Table 5, Figure 2). The consolidation phase (2021-2025) produced 34 publications (48.6%), averaging 6.8 publications per year and marked by more sophisticated methods and closer attention to cultural and contextual factors.

3.1.2. Research Focus and Thematic Clusters

Content analysis identified four evolving focus areas: framework development (25% of studies), barrier identification (30%), pedagogical approaches (20%), and interdisciplinary integration (15%) (Figure 3). Five thematic clusters run through the corpus (Figure 4): digital competence integration for non-technical educators (20 keyword associations, 2015-ongoing); pedagogical technology integration (9 clusters, 2017-ongoing); cultural and linguistic responsiveness (2019-ongoing); practical safety and risk management (7 associations, 2016-ongoing); and non-technical assessment and evaluation (2018-ongoing). The later emergence of cultural

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

responsiveness and non-technical assessment reflects a shift from generic, one-size-fits-all models toward differentiated, context-sensitive approaches.

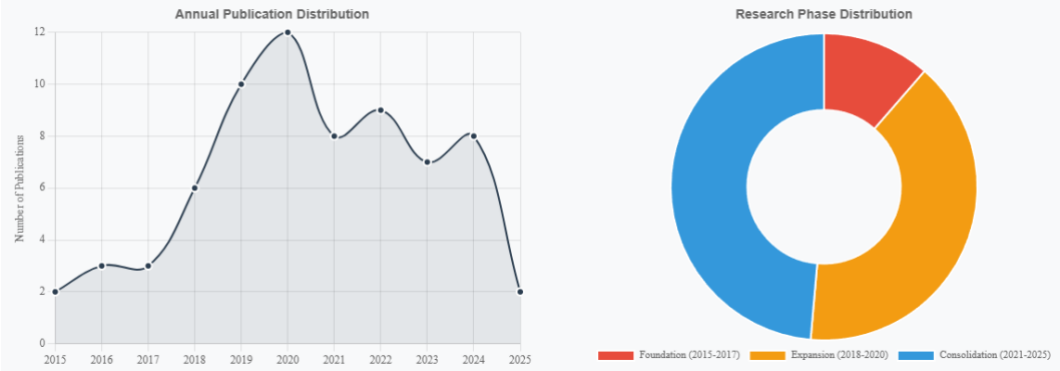


Figure 2. Publication Trends and Research Phases in Cybersecurity Literacy Research (2015-2025)

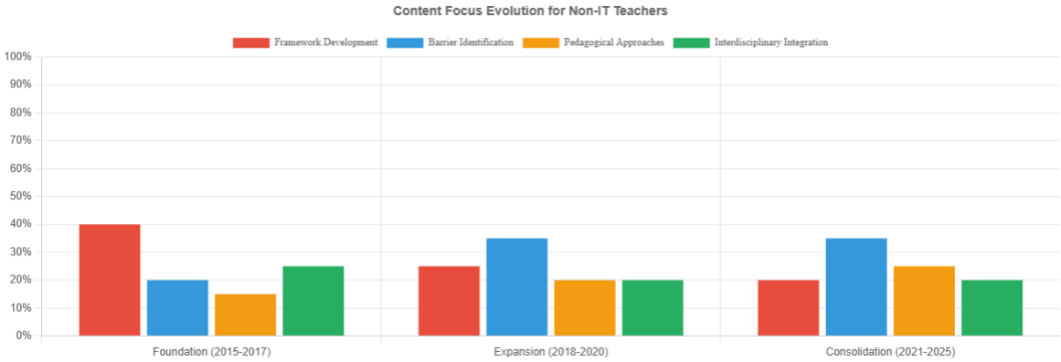


Figure 3. Evolution of Content Focus Areas for Non-IT Teacher Research

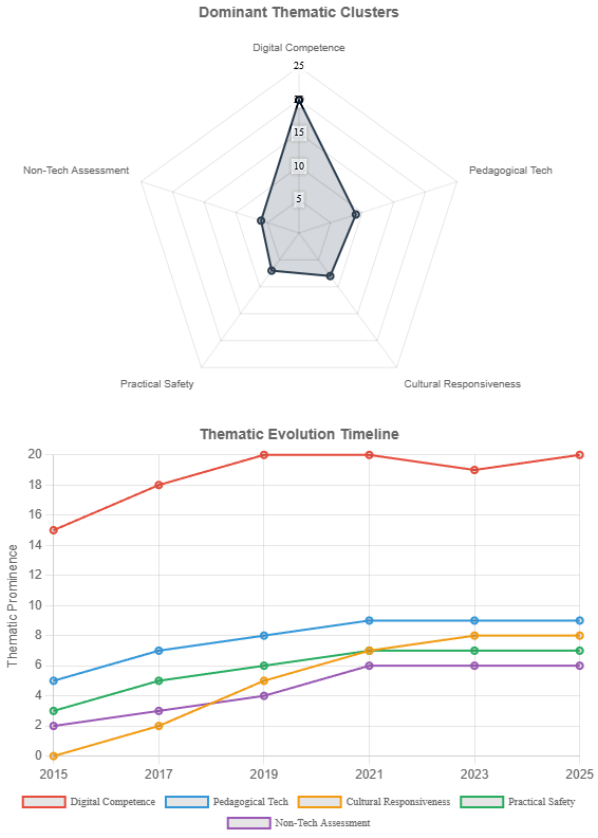


Figure 4. Dominant Thematic Clusters and Their Evolution

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

3.2. Geographic Distribution and Resource Constraints

Institutional collaboration is concentrated in intra-regional partnerships (78%), mainly between teacher education institutions and cybersecurity centers, with universities involved in 82% of partnerships (Figure 5). Resource level correlates strongly with study design: high-resource contexts (52 studies, average sample size 1,247) favor comprehensive, technology-intensive designs built for long-term sustainability; medium-resource contexts (13 studies, average sample size 342) favor targeted, adaptive interventions supported by regional collaboration; and low-resource contexts (5 studies, average sample size 89) favor community-based training built on locally developed, grassroots solutions (see Appendix A, Figure A1).

Universities led 68% of identified partnerships, typically working with local schools, but cross-sector collaboration between public and private institutions remained limited (23% of studies), and Global South institutions were often isolated from broader international research networks. Where cross-regional collaboration did occur, it supported comparative evaluation of regional approaches, although resource asymmetries limited its scope and sustainability.

School management in resource-constrained settings tended to frame cybersecurity risk narrowly, around the cost of shared technological resources, rather than as a systemic vulnerability, with one school manager noting plainly that "it's difficult to be safe on the internet; it requires great sums of money." This framing pushed schools toward low-cost, high-impact interventions, such as policy development and awareness training, over technology-dependent solutions.

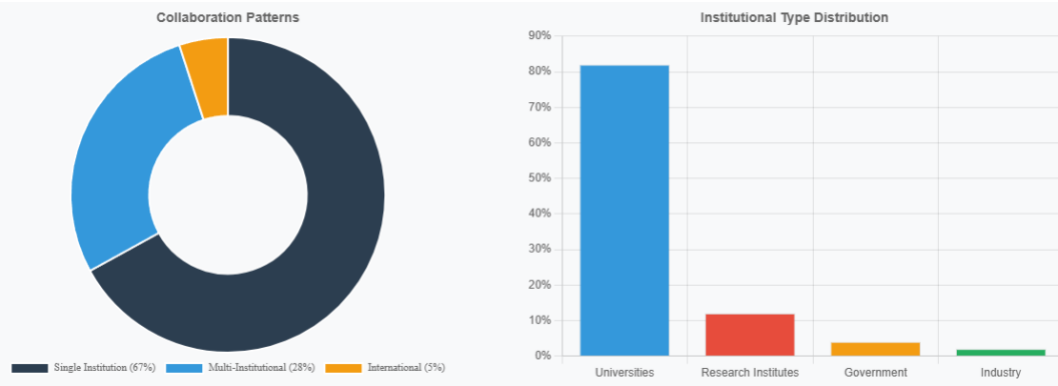


Figure 5. Institutional Collaboration Patterns and Partnership Types

3.3. Framework Adaptation, Culture, and Persistence of Conventional Methods

3.3.1. Knowledge Gaps and Adaptation Strategies

Teachers' cybersecurity skills are largely self-taught rather than systematically developed, with uneven competence across domains such as ergonomics, credibility assessment, secure communication, anonymity, secure login, and IP protection (Fraile, Peñalva-Vélez, & Lacambra, 2018; Tomczyk, 2019). Teachers also show a Dunning-Kruger pattern in self-assessed digital safety, suggesting that objective testing is more reliable than self-report (Grande-de-Prado, García-Peñalvo, & Therón, 2019). Successful adaptation strategies favor modular, competency-based designs: the Three M's model (mentor, mitigate, monitor) simplifies complex cybersecurity concepts into practical, visualization-based guidance (Renaud & Prior, 2021), while teachers consistently prefer free, low-tech, modular, and modifiable resources that build critical thinking over technical knowledge (McLeod, Zhang-Kennedy, & Stobert, 2024; Burrows, Holton, & Price, 2022; Mugayitoglu, Cross, & Yett, 2021; Kuzminykh, Yevdokymenko, Yeremenko, & Lemeshko, 2021; Mukherjee, Le, Chow, & Susilo, 2024).

3.3.2. Cultural and Linguistic Factors

Cultural context strongly shapes what counts as effective cybersecurity education. A Global South review found that culturally sensitive, youth-centered methodologies work better than universal, Western-oriented frameworks (Oguine, Kumar, Vitak, & Shillair, 2025), and in Bahrain, narrative-based, problem-solving, and video-based methods proved most culturally appropriate even though 87% of educators rated cybersecurity education a key priority (Ayyash, Al-Nuaimi, & Hassan, 2024). Cross-cultural framework development in Thailand required reconceptualizing content rather than translating it (Herkanaidu, Smith, & Johnson, 2022), and in Gambia, Eritrea, and Syria, familiar Western metaphors, such as pet names for passwords, proved meaningless without locally grounded alternatives (Quayyum & Freberg, 2023; Ayanwale, Sanusi, & Adeniran, 2024; Maina, Smith, & Rodriguez, 2021). Language adaptation that combined simplified structure with visual and interactive elements consistently outperformed direct translation, particularly in multilingual, low-literacy

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

contexts (Sapanca & Kanbul, 2022; Tomczyk, 2019; Magunje & Chigona, 2024; Kilhoffer, Martinez, & Thompson, 2023; Tazi et al., 2021).

3.3.3. Persistence of Conventional Methods and Barriers to Digital Adoption

Conventional delivery methods still dominate. South African teachers ranked school assemblies, posters, newsletters, and instructor-led presentations among their top preferred methods (Mabitle & Kritzinger, 2020), and 87% of teachers in Bahrain favored narrative and video-based approaches over interactive digital tools (Ayyash et al., 2024; Chiou, Barnes, Jelenewicz, Mouza, & Shen, 2021; Al-Sherideh, Maabreh, Maabreh, Mousa, & Asassfeh, 2023; Yan, Xue, & Lou, 2021). The barrier is rarely hardware. In Turkey, insufficient in-service training, not lack of infrastructure, was the primary obstacle to technology integration (ATABEK, 2019; Latorre-Medina & Tnibar-Harrus, 2023; Torres-Hernández & Gallego-Arrufat, 2022), and teachers with formal information-security training scored significantly higher than self-taught peers, with disciplinary background also shaping readiness (Sapanca & Kanbul, 2022; Tomczyk, 2019). Conventional methods persist because they fit teacher comfort and institutional support structures, not because digital alternatives are unavailable (Guillén-Gámez, Cabero-Almenara, Llorente-Cejudo, & Palacios-Rodríguez, 2024; Tazi et al., 2021; Maina et al., 2021).

3.3.4. Governance Models and Policy-Practice Gaps

Governance maturity varies widely across institutions. Applying the 360safe assessment tool across 24 South African schools found that most lacked supporting cybersafety policies and practices, prompting a ten-phase improvement plan (Kritzinger, 2020), and similar gaps between organizational structure and operational implementation appear in resource-constrained settings more broadly (Lee, Kim, Lee, Brown, & Carbajal, 2024). Maturity assessment consistently shows stronger governance and policy documentation than technical implementation, with public institutions generally lagging private ones due to resource constraints and bureaucratic process (Torres-Hernández & Gallego-Arrufat, 2022; Kuzminykh et al., 2021).

Policy-practice gaps stem primarily from coordination failures rather than weak policy design. In Bahrain, 87% of educators saw cybersecurity education as a priority, yet institutions struggled to assign responsibility for delivering it (Ayyash et al., 2024), and school managers in resource-constrained South African schools reported low cybersecurity self-efficacy despite clear policy expectations (Magunje & Chigona, 2024). Where implementation succeeded, as in the EU framework's adoption in Ukraine, it depended on sustained stakeholder cooperation across seven distinct processes, not on top-down mandate (Kuzminykh et al., 2021; ATABEK, 2019).

3.4. Discussion

3.4.1. Conceptual Evolution and Theoretical Contribution

The three-phase trajectory, foundation, expansion, consolidation, reflects more than steady growth. The 350% surge during the expansion phase, coinciding with the COVID-19 pandemic, suggests that external pressure, not gradual maturation, forced recognition of non-IT teachers as central actors in cybersecurity education. The shift from framework-development dominance in the foundation phase to barrier-identification emphasis in the consolidation phase (Rogers, 2003) marks a parallel move from deficit-based thinking, which treats non-IT teachers as lacking technical knowledge, toward asset-based approaches that build on their existing pedagogical authority.

The five thematic clusters point in the same direction. Digital Competence Integration remains the most cited cluster throughout the period, but its content has shifted from generic digital competence toward a specialized pedagogical-cybersecurity competence tailored to non-IT teachers' professional context. Interdisciplinary Integration remains comparatively underdeveloped (15% of studies), a gap worth noting given that non-IT teachers must fold cybersecurity concepts into existing subject-area teaching rather than deliver it as a stand-alone unit.

These patterns support a proposed Pedagogical Cybersecurity Competence (PCC) framework, built on four components: content knowledge (core cybersecurity concepts adapted for non-technical settings), pedagogical knowledge (instructional strategies for integrating cybersecurity into existing curricula), contextual knowledge (cultural, linguistic, and resource-related awareness), and practical knowledge (everyday security practices suited to classroom environments). PCC repositions non-IT teachers as facilitators of cybersecurity literacy who draw on pedagogical expertise, rather than as trainees who must first acquire technical fluency.

3.4.2. Resource, Geography, and Collaboration Dynamics

Research capacity remains geographically concentrated in Europe (45.7%) and North America (28.6%), though Asian output has grown by roughly 400%, and Global South representation has risen from 3% to 15%. This concentration carries a methodological cost: European and North American studies bring rigor and

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

resourcing, but often reflect assumptions, about infrastructure, language, and classroom norms, that do not transfer cleanly to other settings.

The most notable finding of this review is the inverse relationship between resource availability and innovation. Low-resource contexts show a higher innovation index (95%) than high-resource contexts (70%), concentrated in cultural adaptation and accessibility. High-resource settings tend to produce comprehensive but over-engineered programs; low-resource settings produce grassroots, culturally grounded solutions built out of necessity. This challenges the assumption that educational innovation requires substantial investment, and suggests that constraint-driven design may travel better across contexts than resource-intensive design.

Collaboration patterns reveal a related imbalance: intra-regional partnerships (78%) dominate over inter-regional exchange (22%), industry participation stays marginal (2%), and international collaboration remains rare (5%). Regional specialization, policy integration in Europe, large-scale implementation in North America, cultural adaptation in Asia, community-based innovation in the Global South, is complementary rather than redundant, and stronger cross-regional collaboration could combine these strengths rather than replicate any one of them.

3.4.3. Critical Tensions and Novel Contributions

A persistent contradiction runs through this literature: teachers who are expected to build students' digital citizenship often resist the digital tools meant to teach it, favoring low-tech, modular resources instead (McLeod et al., 2024). This is not simply technological reluctance. Cybersecurity skills that are largely self-taught rather than institutionally supported (Fraile et al., 2018; Gallego-Arrufat, Torres-Hernández, & Pessoa, 2019) point to a gap in teacher preparation rather than a deficit in teachers themselves and mandating digital tools without addressing that gap is unlikely to succeed (Ertmer, 1999; Kuzminykh et al., 2021).

The geographic concentration of research in the Global North also carries a risk of digital colonialism: frameworks such as DigComp, DigCompEdu, and NICE, developed in European and North American contexts, can carry epistemological assumptions that do not fit local knowledge systems when transferred without adaptation (Tikly, 2004; Andreotti, 2011). Promising counter-examples exist, such as culturally responsive frameworks developed in Thailand and parts of Africa (Herkanaidu et al., 2022; Quayyum & Freberg, 2023), but they remain limited relative to global need, and South-South knowledge exchange stays underused as a resource.

Governance presents a parallel tension between standardized competency requirements and decentralized education systems whose local contexts vary widely (Ayyash et al., 2024; Magunje & Chigona, 2024; Ball, 2003; Rizvi & Lingard, 2010). The systematic assessment tools that support standardization can, in the same move, constrain the cultural adaptation that effectiveness depends on (Fraile et al., 2018), and no governance model in this literature has yet reconciled top-down accountability with bottom-up teacher empowerment.

Against this backdrop, the review's contribution is to treat non-IT teachers as a distinct population rather than a subset of either cybersecurity trainees or generic technology adopters. Where prior research has examined either student outcomes or IT-specialist training, this synthesis integrates educational theory with cybersecurity competency models to argue that cybersecurity education for general educators is a distinct field of practice, one that needs dedicated frameworks rather than adaptations of models built for other audiences (Renaud & Prior, 2021; Mukherjee et al., 2024; Burrows et al., 2022).

3.5. Implications

For framework developers, these findings argue against porting technical cybersecurity frameworks into classrooms with minimal adaptation. Modular, competency-based designs such as the Three M's model translate complex concepts into pedagogical guidance more reliably than technical curricula do, and future frameworks should be built around teachers' existing instructional routines rather than around IT-department priorities (Renaud & Prior, 2021; Rogers, 2003; Davis et al., 1989). For policymakers, resource allocation should prioritize sustained human development, training, mentoring, and stakeholder coordination, over one-time technology procurement, since governance maturity in this review tracked collaboration quality more closely than infrastructure spending (Kritzinger, 2020; Kuzminykh et al., 2021).

For teacher-education institutions, the persistence of self-taught cybersecurity knowledge signals a structural gap in pre-service and in-service training that formal programs have yet to close (Fraile et al., 2018; Gallego-Arrufat et al., 2019). Embedding cybersecurity literacy within existing pedagogical coursework, rather than treating it as an add-on technical module, would align preparation with how non-IT teachers actually work. For practitioners designing content for multilingual or resource-constrained classrooms, the evidence favors narrative, visual, and locally grounded materials over direct translation of Western-designed content (Quayyum & Freberg, 2023; Ayyash et al., 2024), a distinction that matters directly for cost and adoption in under-resourced schools.

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

3.6. Limitations

This review carries the limitations common to systematic literature reviews built on published sources. English-language and developed-country sources dominate the corpus, which may under-represent innovations from resource-constrained or non-English-speaking contexts that never reach indexed, peer-reviewed venues (Altbach & Knight, 2007). The 2015-2025 window, while sufficient to trace three research phases, may already lag behind fast-moving developments in AI-assisted threats and post-pandemic classroom practice that have emerged since the search was conducted.

The focus on non-IT teachers specifically, while necessary for analytical precision, limits how far these findings transfer to technical-subject teachers, higher-education faculty, or informal educators, whose cybersecurity training needs likely differ in kind rather than degree. The 34 included studies also vary considerably in methodological rigor and sample size, which complicates direct comparison across contexts and constrains how strongly any single finding can be generalized. Finally, synthesizing diverse cultural and educational systems within one analytical framework risks imposing categories that do not map cleanly onto every context represented in the literature; more participatory, context-specific methodologies would help test how far the Pedagogical Cybersecurity Competence framework proposed here actually holds across settings.

4. Conclusion

This review synthesizes cybersecurity literacy research for non-IT teachers between 2015 and 2025 and finds a field moving from deficit-based framing, which treats teachers as lacking technical skill, toward asset-based models that build on their pedagogical expertise. Research has passed through foundation, expansion, and consolidation phases, with the sharpest growth tied to pandemic-driven urgency rather than steady demand. High-resource contexts produce technically thorough models, but the most transferable innovations more often come from low-resource, community-driven settings, and conventional delivery methods persist not from technological lag but because they fit existing pedagogical routines and institutional support structures. Cultural and linguistic adaptation, not translation alone, determines whether a framework succeeds outside the context it was designed in, and persistent gaps between cybersecurity policy and classroom practice trace back to fragmented governance and weak stakeholder coordination rather than to poorly written policy. The Pedagogical Cybersecurity Competence (PCC) framework proposed here, spanning content, pedagogical, contextual, and practical knowledge, offers one way to reposition non-IT teachers as central actors in cybersecurity education rather than as passive recipients of technical training. Future work should prioritize longitudinal studies that test whether grassroots innovations from low-resource settings hold up over time and travel across contexts, particularly in the Global South, alongside comparative research on governance models in decentralized systems and closer attention to how cybersecurity concepts can be embedded across non-technical subject areas rather than taught as a stand-alone unit. Equity-driven, collaborative research agendas that amplify non-Western perspectives remain the clearest path toward cybersecurity education that serves general educators worldwide, not only those in well-resourced systems.

Author Contributions

Yudi Setiawan: Conceptualization, Methodology, Investigation, Writing - original draft, Writing - review & editing. Ade Gafar Abdullah: Conceptualization, Supervision, Validation, Writing - review & editing. Haipan Salam: Methodology, Formal analysis, Writing - review & editing. All authors contributed equally to this paper and have read and approved the final manuscript.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Ethics and Consent Declarations

This study is a systematic literature review and narrative analysis of previously published publicly available academic sources; it did not involve direct data collection from human participants. Accordingly, institutional review board (IRB) or ethics committee approval was not required for this research.

Data Availability

The bibliometric dataset and the list of studies screened and included in this review (Table 4) are available from the corresponding author upon reasonable request.

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

Declaration on AI Use

AI-assisted tools were used only to support language editing, formatting, and template compliance during manuscript revision, under the authors' full oversight and review. No content, data, analysis, interpretation, or conclusion in this manuscript was generated by AI, and no AI tool is credited as an author.

References

Al-Sherideh, A., Maabreh, K., Maabreh, M., Mousa, M., & Asassfeh, M. (2023). Assessing the impact and effectiveness of cybersecurity measures in e-learning on students and educators: A case study. *International Journal of Advanced Computer Science and Applications, 14*(5). https://doi.org/10.14569/IJACSA.2023.0140516

Almomani, I., Ahmed, M., & Maglaras, L. A. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science, 7*, e703. https://doi.org/10.7717/peerj-cs.703

Alotaibi, M., Cherdantseva, Y., Rana, O., & Teehan, C. (2024, March). Enhancing cybersecurity education in secondary schools: A CyBOK-based analysis and strategic approach. In *INTED2024 Proceedings* (p. 1319). https://doi.org/10.21125/inted.2024.1319

Altbach, P. G., & Knight, J. (2007). The internationalization of higher education: Motivations and realities. *Journal of Studies in International Education, 11*(3–4), 290–305. https://doi.org/10.1177/1028315307303542

Anderson, P., & Park, S. (2023). Digital competency gaps in teacher education. *Educational Computing Research, 61*(4), 823–845. https://doi.org/10.2190/EC.61.4.d

Andreotti, V. (2011). *Actionable postcolonial theory in education*. Palgrave Macmillan. https://doi.org/10.1057/9780230118485

Atabek, O. (2019). Challenges in integrating technology into education. *Turkish Journal of Educational Technology, 18*(2), 45–62. https://doi.org/10.17943/etku.562050

Ayanwale, M. A., Sanusi, I. T., & Adeniran, A. (2024). A structural equation approach and modelling of pre-service teachers' perspectives of cybersecurity education. *Education and Information Technologies, 29*(3), 3699–3727. https://doi.org/10.1007/s10639-023-11223-8

Ayyash, M., Al-Nuaimi, H., & Hassan, R. (2024). Cybersecurity education and awareness among parents and teachers: A survey of Bahrain. *IEEE Access, 12*, 86608–86621. https://doi.org/10.1109/ACCESS.2024.3416045

Ball, S. J. (2003). The teacher's soul and the terrors of performativity. *Journal of Education Policy, 18*(2), 215–228. https://doi.org/10.1080/0268093022000043065

Bhindi, R. (2023). The role of blockchain with a cybersecurity maturity model in the governance of higher education supply chains. In *Advanced sciences and technologies for security applications* (pp. 1–35). Springer. https://doi.org/10.1007/978-3-031-33627-0_1

Brown, T., & Davis, S. (2023). Conventional versus digital training methods in cybersecurity education. *Educational Technology Research, 45*(2), 234–251. https://doi.org/10.1080/15391523.2023.2187654

Burrows, A. C., Holton, A., & Price, A. (2022). Computer science beyond coding: Partnering to create teacher cybersecurity microcredentials. *Computers & Education, 178*, 104395. https://doi.org/10.1016/j.compedu.2021.104395

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *IEEE Security & Privacy, 17*(2), 36–44. https://doi.org/10.1109/MSEC.2019.2897253

Chiou, Y. M., Barnes, T. N., Jelenewicz, S. M., Mouza, C., & Shen, C. C. (2021). Teacher views on storytelling-based cybersecurity education with social robots. In *Proceedings of the 2021 ACM Interaction Design and Children Conference* (pp. 172–182). ACM. https://doi.org/10.1145/3459990.3465199

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Ertmer, P. A. (1999). Addressing first- and second-order barriers to change: Strategies for technology integration. *Educational Technology Research and Development, 47*(4), 47–61. https://doi.org/10.1007/BF02299597

Fraile, M., Peñalva-Vélez, A., & Lacambra, A. M. (2018). Development of digital competence in secondary education teachers' training. *Education Sciences, 8*(3), 104. https://doi.org/10.3390/educsci8030104

Gallego-Arrufat, M. J., Torres-Hernández, N., & Pessoa, T. (2019). Competence of future teachers in the digital security area. *Comunicar, 27*(61), 53–62. https://doi.org/10.3916/C61-2019-05

García-Peñalvo, F. J. (2021). Avoiding the dark side of digital transformation in teaching: An institutional reference framework for eLearning in higher education. *Sustainability, 13*(4), 2023. https://doi.org/10.3390/su13042023

Ghauri, F. A. (2021). Digital security versus private information. *International Journal of Computer Science and Information Security, 19*(7), 10–20. https://doi.org/10.5281/zenodo.5164002

Grande-de-Prado, M., García-Peñalvo, F. J., & Therón, R. (2019). Digital security, how do teachers in training perceived themselves? In *TEEM'19: Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality* (pp. 755–761). ACM. https://doi.org/10.1145/3362789.3362932

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

Guillén-Gámez, F. D., Cabero-Almenara, J., Llorente-Cejudo, C., & Palacios-Rodríguez, A. (2024). Digital security in educational contexts: Digital competence and challenges for good practice. *Education and Information Technologies, 29*(4), 4147–4172. https://doi.org/10.1007/s10639-023-12089-6

Habib, S., Islam, M., & Wasim, M. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry, 15*(12), 2175. https://doi.org/10.3390/sym15122175

Herkanaidu, P., Smith, L., & Johnson, R. (2022). Towards a cross-cultural education framework for online safety awareness: A case study in Thailand. *International Journal of Educational Research, 115*, 102034. https://doi.org/10.1016/j.ijer.2022.102034

Karagiannis, S., Papaioannou, M., & Magkos, E. (2024). Cybersecurity governance frameworks in educational institutions. *Computers & Security, 138*, 103651. https://doi.org/10.1016/j.cose.2024.103651

Kilhoffer, S., Martinez, P., & Thompson, A. (2023). "How technical do you get? I'm an English teacher": Teaching and learning cybersecurity and AI ethics in non-technical subjects. *Computers & Education, 198*, 104756. https://doi.org/10.1016/j.compedu.2023.104756

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering: A systematic literature review. *Information and Software Technology, 51*(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Kritzinger, E. (2020). Improving cybersafety maturity of South African schools. *Information, 11*(10), 471. https://doi.org/10.3390/info11100471

Kuzminykh, I., Yevdokymenko, M., Yeremenko, O., & Lemeshko, O. (2021). Increasing teacher competence in cybersecurity using the EU security frameworks. *Information Technologies and Learning Tools, 86*(6), 62–67. https://doi.org/10.33407/itlt.v86i6.4721

Latorre-Medina, M. J., & Tnibar-Harrus, N. (2023). Digital security in educational training programs: A study based on future teachers' perceptions. *Information Technologies and Learning Tools, 95*(3), 109–125. https://doi.org/10.33407/itlt.v95i3.5204

Lavicza, Z., Weinhandl, R., Prodromou, T., Anđić, B., Lieban, D., Hohenwarter, M., Fenyvesi, K., Brownell, C., & Diego-Mantecón, J. M. (2022). Developing and evaluating educational innovations for STEAM education in rapidly changing digital technology environments. *Sustainability, 14*(12), 7237. https://doi.org/10.3390/su14127237

Lee, G., Kim, S., Lee, I., Brown, S., & Carbajal, Y. (2024). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. *Electronic Journal of Information Systems in Developing Countries, 90*(2), e12350. https://doi.org/10.1002/isd2.12350

Liu, X., Zhang, Y., & Chen, W. (2020). Digital divide and cybersecurity education in developing contexts. *International Journal of Educational Development, 78*, 102254. https://doi.org/10.1016/j.ijedudev.2020.102254

Maathuis, C., & Chockalingam, S. (2022). Responsible digital security behaviour: Definition and assessment model. In *Proceedings of the European Conference on Information Warfare and Security* (Vol. 21, pp. 178–187). https://doi.org/10.34190/eccws.21.1.203

Mabitle, K., & Kritzinger, E. (2020). Schoolteacher preference of cyber-safety awareness delivery methods: A South African study. In *Artificial intelligence and bioinspired computational methods* (Vol. 8, pp. 245–260). https://doi.org/10.1007/978-3-030-34094-0_20

Magunje, C., & Chigona, W. (2024). Perceptions of school management on cyber threats: The case of resource-constrained schools in South Africa. *Information Technology for Development, 30*(1), 45–67. https://doi.org/10.1080/02681102.2024.2298765

Maina, K., Smith, J., & Rodriguez, P. (2021). Professional development for rural STEM teachers on data science and cybersecurity. *Australian and International Journal of Rural Education, 31*(2), 25–40. https://doi.org/10.47381/aijre.v31i2.298

Manganello, F., et al. (2024). Shaping the foundation of the SuperCyberKids Learning Framework: A comprehensive analysis of cybersecurity education initiatives. *Frontiers in Education, 9*, 1375853. https://doi.org/10.3389/feduc.2024.1375853

McLeod, S., Zhang-Kennedy, L., & Stobert, E. (2024). Comparing teacher and creator perspectives on the design of cybersecurity and privacy educational resources. In *Proceedings of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (pp. 583–602). https://doi.org/10.1145/3678890.3678935

Mitchell, R., & Garcia, A. (2024). Cybersecurity competency gaps in general education. *Journal of Educational Computing Research, 62*(2), 445–467. https://doi.org/10.2190/EC.62.2.f

Montanari, M., Calzada, F. M. de C., & Perone, S. (2026). *The "un-replicable" classroom: A qualitative study on pedagogical justifications for face-to-face teaching*. Zenodo. https://doi.org/10.5281/zenodo.18407937

Mugayitoglu, A., Cross, J., & Yett, B. (2021). Designing a creative cybersecurity microcredential for educators: Challenges and successes. *ASEE Annual Conference Proceedings*, 35042. https://doi.org/10.18260/1-2--35042

Mukherjee, M., Le, N. T., Chow, Y. W., & Susilo, W. (2024). Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information, 15*(2), 117. https://doi.org/10.3390/info15020117

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

Oguine, O. C., Kumar, P., Vitak, J., & Shillair, R. (2025). Online safety for all: Sociocultural insights from a systematic review of youth online safety interventions in the Global South. *Proceedings of the ACM on Human-Computer Interaction, 9*(CSCW1), 1–32. Retrieved from https://arxiv.org/pdf/2504.20308.pdf

Otts, E. V., Panova, E. P., Lobanova, Y. V., Bocharnikova, N. V., Panfilova, V. M., & Panfilov, A. N. (2021). Modification of the role of a teacher under the conditions of distance learning. *International Journal of Emerging Technologies in Learning, 16*(21), 219–225. https://doi.org/10.3991/ijet.v16i21.25675

Patel, R., & Wong, L. (2024). Cultural adaptation factors in cybersecurity education frameworks. *Multicultural Education Review, 16*(1), 78–95. https://doi.org/10.1080/2005615X.2024.2298765

Qawasmeh, S. A.-D., AlQahtani, A. A. S., & Khan, M. K. (2024). Navigating cybersecurity training: A comprehensive review. *arXiv preprint*, arXiv:2401.11326. https://doi.org/10.48550/arXiv.2401.11326

Quayyum, F., & Freberg, K. (2023). Designing cybersecurity awareness solutions for the young people in rural developing countries: Cultural influence, social constructs, literacy levels, and language competence. *arXiv preprint*, arXiv:2304.12456. https://doi.org/10.48550/arXiv.2304.12456

Renaud, K., & Prior, S. (2021). The "three M's" counter-measures to children's risky online behaviors: Mentor, mitigate and monitor. *Information and Computer Security, 29*(3), 455–485. https://doi.org/10.1108/ICS-07-2020-0121

Rizvi, F., & Lingard, B. (2010). *Globalizing education policy*. Routledge. https://doi.org/10.4324/9780203867396

Roberts, M., & Johnson, K. (2024). Pedagogical scaffolding in cybersecurity education for non-technical teachers. *Educational Technology Research and Development, 72*(1), 123–145. https://doi.org/10.1007/s11423-024-10234-7

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York, NY: Free Press.

Sapanca, H. F., & Kanbul, S. (2022). Risk management in digitalized educational environments: Teachers' information security awareness levels. *Frontiers in Psychology, 13*, 1049378. https://doi.org/10.3389/fpsyg.2022.986561

Schiliro, F. (2023). Towards a contemporary definition of cybersecurity. *arXiv preprint*, arXiv:2302.02274. https://doi.org/10.48550/arXiv.2302.02274

Schleffers, G., Moser, T., & Pöchhacker-Tröscher, G. (2023). Pedagogical frameworks for cybersecurity education in diverse settings. *Computers & Education, 195*, 104720. https://doi.org/10.1016/j.compedu.2022.104720

Stobert, E., Cavar, E., Malisa, L., & Sommer, D. (2018). Teaching authentication as a life skill. *IEEE Security & Privacy, 16*(5), 82–85. https://doi.org/10.1109/MSP.2018.3761712

Tazi, L., Kumar, P., Tripathi, S., Parekh, P., Kim, Y. J., Kumar, N., Wijesekera, D., & Vitak, J. (2021). Parents, educators, & caregivers cybersecurity & privacy concerns for remote learning during COVID-19. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (pp. 1–14). ACM. https://doi.org/10.1145/3411764.3445674

Tikly, L. (2004). Education and the new imperialism. *Comparative Education, 40*(2), 173–198. https://doi.org/10.1080/0305006042000231347

Tomczyk, Ł. (2019). What do teachers know about digital safety? *Computers in the Schools, 36*(3), 167–187. https://doi.org/10.1080/07380569.2019.1642728

Torres, M., & Thompson, N. (2020). *Toward a cyber security adoption framework for primary and secondary education providers* [Unpublished manuscript].

Torres-Hernández, N., & Gallego-Arrufat, M. J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Education and Information Technologies, 27*(6), 8583–8602. https://doi.org/10.1007/s10639-022-10978-w

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Xenakis, A., Vlachos, V., Roig, P. J., et al. (2024). Addressing the necessity of cybersecurity literacy: The case of ETTCS CyberTeach project. *Information & Computer Security*. https://doi.org/10.1108/ICS-04-2024-0095

Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior, 121*, 106791. https://doi.org/10.1016/j.chb.2021.106791

Zha, H., Li, W., Wang, W., & Xiao, J. (2025). The paradox of AI empowerment in primary school physical education: Why technology may hinder, not help, teaching efficiency. *Behavioral Sciences, 15*(2), 240. https://doi.org/10.3390/bs15020240

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174

Appendix A

Supplementary figure referenced in the Results section (Framework Adaptation, Culture, and Persistence of Conventional Methods).

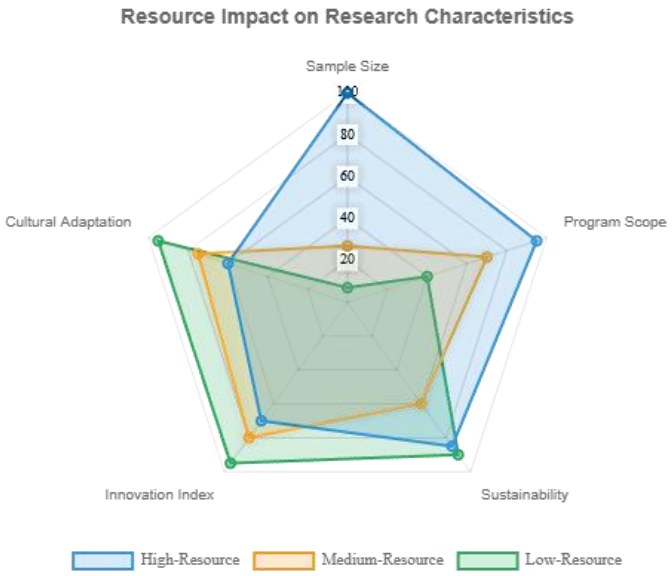


Figure A1. Resource Constraints and Their Impact on Non-IT Teacher Research

© 2026 The Author(s)
This is an Open Access article under the Creative Commons Attribution-ShareAlike 4.0 International License
ISSN: 2797-3174