SITEKNIK
Sistem Informasi, Teknik dan Teknologi Terapan
E-ISSN: 3032-3991 P-ISSN: 3090-1626
Vol. 3, No. 2 April 2026. Pages. 61-68

From Technical Security to Human Awareness: A Bibliometric Review of Cybersecurity Education Research

Cindy Muhdiantini[1]✉, Mega Fitri Yani[2], Istifa Shania Putri[3]
cindymuhdiantinicm@telkomuniversity.ac.id[1], megafy@telkomuniversity.ac.id[2], istifashaniaputri@telkomuniversity.ac.id[3]
[123] Information System, Faculty of Industrial Engineering, Telkom University, Indonesia

Keywords: Cybersecurity Education, Bibliometric Analysis, Security Awareness, Research Trends

Submitted: 16/04/2026
Revised: 28/04/2026
Accepted: 29/04/2026

Abstract

The rapid advancement of information technology has increased cybersecurity threats, emphasizing the importance of education in building security awareness and human-centered defense capabilities. As research on cybersecurity education continues to grow, a systematic understanding of its research trends and thematic evolution is required. This study analyzes global research trends in cybersecurity education using a bibliometric approach. A total of 189 Scopus-indexed publications from 2020 to 2026 were analyzed using the *bibliometrix* R package and the Biblioshiny interface. The analysis examines annual publication growth, dominant keywords, evolving research topics, and geographical research contributions. The results indicate a steady increase in scientific production, confirming cybersecurity education as an expanding research domain. While technical topics such as network and data security remain prominent, recent research shows a clear shift toward education, training, and security awareness, highlighting the growing importance of human factors in cybersecurity. In addition, the findings reveal an imbalance in global research contributions and relatively limited international collaboration. This study provides a concise overview of the development and structure of cybersecurity education research and offers insights to support future studies, curriculum development, and policy formulation.

Corresponding Author:
Cindy Muhdiantini[1]✉
Information System, Faculty of Industrial Engineering, Telkom University
Jl. Telekomunikasi No.1, Bandung
Email: cindymuhdiantinicm@telkomuniversity.ac.id

INTRODUCTION

The rapid advancement of information technology has significantly increased society's reliance on digital systems across various sectors, including education, government, industry, and public services. Along with this increased dependence, cybersecurity threats have escalated in both complexity and impact. Cyberattacks, data breaches, and information misuse have become critical challenges that require attention

beyond technical solutions alone, extending to human and organizational factors (Ahmed et al., 2023; Al-Badayneh et al., 2025; De Bruin & Mersinas, 2022).

Cybersecurity has therefore become a critical concern in modern digital environments due to the increasing frequency, scale, and sophistication of cyber threats (Admass et al., 2024; Qureshi & Koo, 2026). The rapid expansion of digital technologies, cloud services, and interconnected systems has increased the attack surface, making individuals, organizations, and societies more vulnerable to cyber incidents. Early cybersecurity research predominantly concentrated on technical solutions, including network security mechanisms, cryptographic techniques, intrusion detection systems, and system hardening strategies.

However, subsequent studies have demonstrated that purely technical solutions are insufficient to fully address cybersecurity challenges, particularly those rooted in human behavior and organizational practices (Khadka & Ullah, 2025). Issues such as weak passwords, phishing susceptibility, poor security decision-making, and inadequate security culture have been identified as major contributors to security breaches (Kennison & Chan-Tin, 2020; Ngandu et al., 2025; Oner et al., 2025). These findings highlight that cybersecurity is not solely a technical problem but also a socio-technical issue that requires attention to human, educational, and organizational dimensions.

In response to these challenges, cybersecurity education has emerged as a critical approach to strengthening cybersecurity resilience. Cybersecurity education is not only intended to develop skilled cybersecurity professionals but also to enhance security awareness among general users of information systems (Ahmed Shan-A-Alahi, 2024; Prümmer et al., 2024; Shillair et al., 2022; Temitayo Oluwaseun Abrahams et al., 2024). By fostering awareness, competencies, and responsible behavior, cybersecurity education plays a strategic role in reducing security risks at the user level and supporting a sustainable information security culture. Well-designed curricula, effective learning methods, and appropriate educational approaches are therefore essential for supporting secure digital ecosystems (Fida Hasan et al., 2025).

As the importance of cybersecurity education has increased, scientific publications in this field have grown significantly. Existing studies cover a wide range of topics, including curriculum development, information security awareness, cybersecurity training, and the integration of cybersecurity into formal and non-formal education (Arishia et al., 2024; Fida Hasan et al., 2025; Shillair et al., 2022). This growth reflects the increasing recognition of education as a preventive and long-term cybersecurity strategy.

However, the rapid expansion of publications creates challenges in understanding the overall research landscape. It becomes difficult to identify dominant research themes, track the evolution of research topics, and determine gaps in the literature comprehensively. Moreover, previous bibliometric studies on cybersecurity have primarily focused on technical domains such as intrusion detection, cryptography, malware analysis, and network security (Ngandu et al., 2025; Sharma et al., 2023; Singh et al., 2025), while educational, behavioral, and security awareness aspects remain relatively underexplored (Verma et al., 2025).

To address this gap, a systematic approach is required to map and analyze the development of cybersecurity education research. Bibliometric analysis provides an effective method for examining the intellectual structure of a research field through the analysis of scientific publications, keywords, topic trends, and geographical research contributions (Kumar, 2025; Passas, 2024; Verma et al., 2025).

Therefore, this study aims to analyze research trends in cybersecurity education using a bibliometric approach supported by the Biblioshiny tool. Specifically, this study examines publication growth over time, identifies the most frequently occurring keywords and major research themes, and maps global research contributions. The findings are expected to provide a comprehensive overview of cybersecurity education research and

serve as a reference for researchers, educators, and policymakers in shaping future research directions and educational strategies in cybersecurity.

RESEARCH METHODS

Data Collection

This study employed a bibliometric approach to systematically analyze global research trends related to cybersecurity education and user awareness. Bibliometric analysis was selected because it enables quantitative assessment of large volumes of scientific publications and facilitates the identification of research patterns, thematic developments, and geographical contributions. Publication data were retrieved from the Scopus Core Collection database, which was chosen due to its broad coverage of high-quality, peer-reviewed international journals and conference proceedings in the fields of information technology and computer science.

Data extraction was conducted using a TITLE-ABS-KEY search strategy to ensure that the retrieved documents were directly relevant to the research focus. The search query combined cybersecurity-related terms ("information security" OR "cybersecurity" OR "cyber security") with education-related terms (education OR training OR learning OR curriculum) and security awareness-related terms (awareness OR "security awareness" OR "user awareness" OR "human factor"). To capture recent research developments and emerging trends, the publication period was limited to 2020–2026. The final search resulted in 189 relevant documents, and all bibliographic data were exported in RIS format to support compatibility with bibliometric analysis tools.

Bibliometric Analysis

The bibliometric analysis was performed using the bibliometrix R package and its web-based interface, Biblioshiny, which provide comprehensive functionalities for bibliometric data processing, analysis, and visualization. These tools enable efficient exploration of publication metadata, including authorship, keywords, publication years, and country affiliations.

The analysis focused on several key indicators to provide an overview of research dynamics in cybersecurity education and user awareness. Key analyses included Annual scientific production, most relevant words, trend topics, corresponding author's countries.

This approach provides a systematic overview of global research dynamics in cybersecurity education and user awareness.

RESULTS AND DISCUSSION

Growth of Scientific Production in Cybersecurity Education

The Annual Scientific Production analysis illustrates the temporal distribution of publications related to cybersecurity education. As shown in Figure. 1, the number of articles published annually remains relatively low and fluctuates during the early years of the observed period, indicating limited research activity in the initial stage of the field.

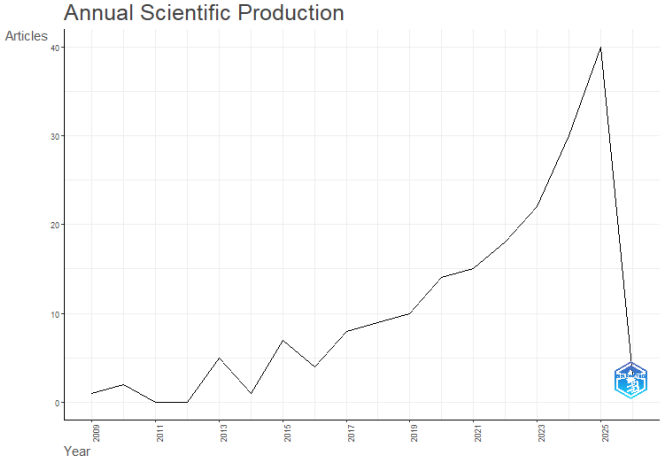

Figure 1. Annual Scientific Production

Beginning around the mid-2010s, a gradual increase in publication output can be observed, followed by a more pronounced upward trend in subsequent years. The number of publications rises steadily, reaching its peak in the most recent complete year of the dataset. This pattern indicates a growing and sustained research interest in cybersecurity education over time.

The sharp decline observed in the final year is likely attributable to the partial coverage of publications for that year in the dataset, rather than a genuine decrease in research activity. Such a pattern is commonly observed in bibliometric analyses when the most recent year has not yet been fully indexed.

Overall, the increasing trajectory of annual scientific production suggests that cybersecurity education has evolved into an increasingly important research domain. The observed growth aligns with the rising global concern over cyber threats, data breaches, and the demand for skilled cybersecurity professionals. These factors have contributed to greater academic attention on educational strategies, curriculum development, and training initiatives aimed at strengthening cybersecurity capabilities.

Core Research Themes and Knowledge Structure

The analysis of Most Relevant Words reveals the dominant research themes in cybersecurity education literature based on keyword occurrences. As shown in Figure. 2, the terms “cyber security” and “cybersecurity” appear most frequently, with 111 and 102 occurrences, respectively. This dominance indicates that research in this domain is strongly centered on cybersecurity as a core concept, although variations in terminology are still evident across publications.

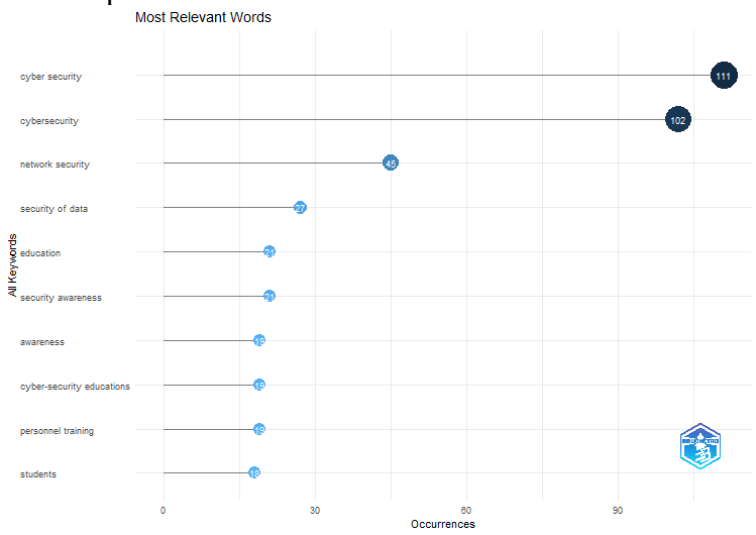

Figure 2. Most Relevant Words

The high frequency of “network security” (45 occurrences) and “security of data” (27 occurrences) suggests that educational research in cybersecurity remains closely connected to traditional technical foundations. These topics reflect the emphasis on protecting network infrastructures and data assets, which continue to form the backbone of cybersecurity curricula and training programs.

In addition to technical terms, keywords related to educational aspects such as “education” (24 occurrences) and “security awareness” (23 occurrences) appear with notable frequency. This finding indicates that the literature increasingly acknowledges the role of education and awareness in addressing cybersecurity challenges. The presence of these terms highlights a shift toward integrating cybersecurity concepts into structured educational frameworks rather than treating them solely as technical competencies.

Furthermore, the appearance of keywords such as “awareness,” “cyber-security educations,” “personnel training,” and “students” each with comparable occurrence levels underscores the growing focus on human factors in cybersecurity. These terms reflect

research efforts aimed at improving user behavior, training effectiveness, and student preparedness in cybersecurity contexts.

Overall, the keyword distribution demonstrates that cybersecurity education research is characterized by a combination of technical security foundations and human-centered educational approaches. While core security concepts continue to dominate the literature, the increasing visibility of education-, awareness-, and training-related terms suggests a gradual transition toward a more holistic understanding of cybersecurity, where technical solutions are complemented by effective education and capacity building.

Evolution of Research Topics Over Time

The Trend Topics analysis illustrates the temporal evolution of research themes in cybersecurity education over the analyzed period, as presented in Figure. 3. The horizontal timelines indicate the duration and intensity of each topic's appearance in the literature, while the size of the markers reflects term frequency.

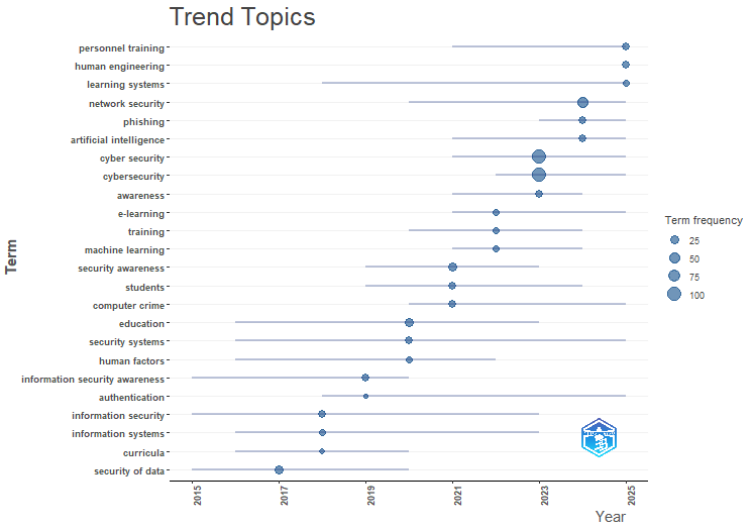

Figure 3. Trend Topics

Early research is primarily characterized by foundational security topics such as security of data, information security, and information systems, which appear consistently during the earlier years of the dataset. These topics reflect the initial technical orientation of cybersecurity-related research, where the primary focus was on protecting data and information systems.

Beginning in the mid-2010s, the emergence of terms such as curricula, education, students, and computer crime indicates a gradual shift toward educational and institutional perspectives. This transition suggests that researchers increasingly recognized the importance of structured education and academic programs in addressing cybersecurity challenges.

In more recent years, topics related to security awareness, human factors, and training gain prominence, highlighting a growing emphasis on human-centered cybersecurity approaches. The appearance and persistence of these topics suggest an acknowledgment that user behavior and awareness play a critical role in the effectiveness of security measures.

Global Contribution and Collaboration Patterns

The analysis of Corresponding Author's Countries provides insight into the geographical distribution and collaboration patterns of cybersecurity education research. As shown in Figure. 4, research output is dominated by a limited number of countries, with Germany and the United States contributing the highest number of corresponding author publications. These countries exhibit a substantial volume of both single-country publications (SCP) and multiple-country publications (MCP), indicating strong national research capacity combined with active international collaboration.

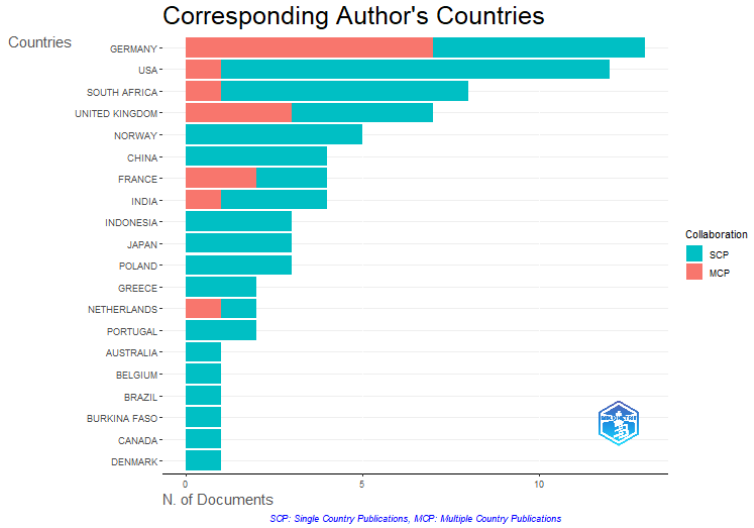

Figure 4. Corresponding Author's Countries

Other countries such as South Africa, the United Kingdom, and Norway also demonstrate notable research contributions, although with lower publication counts compared to the leading countries. The presence of both SCP and MCP in these countries suggests varying degrees of engagement in international research collaboration.

In contrast, several countries including China, India, Indonesia, Japan, and Poland show research outputs that are predominantly characterized by single-country publications. This pattern indicates that cybersecurity education research in these countries is largely conducted within national boundaries, with limited cross-country collaboration. Possible contributing factors include differences in research funding structures, language barriers, and varying levels of integration into global research networks.

The overall distribution highlights a geographical imbalance in global research contributions, where countries with established cybersecurity infrastructures and academic ecosystems tend to dominate the field. While international collaboration is present, as reflected by the MCP values, the dominance of SCP across many countries suggests that global collaboration in cybersecurity education remains relatively limited.

These findings imply that there is significant potential to enhance international research cooperation in cybersecurity education. Strengthening cross-border collaborations could facilitate the exchange of best practices, support comparative studies, and contribute to the development of cybersecurity education frameworks that are globally informed yet locally adaptable. Such efforts may also help reduce disparities in research contributions and promote a more inclusive global research landscape.

CONCLUSIONS AND SUGGESTIONS

Conclusion

This study provides a bibliometric overview of research trends in cybersecurity education, highlighting its growth, thematic evolution, and global research distribution. The findings indicate a consistent increase in scientific production, confirming that cybersecurity education has become an increasingly important research domain.

The analysis reveals that, while the field remains rooted in technical security concepts, there is a significant shift toward educational, awareness-based, and human-centered approaches. This shift reflects a broader understanding that effective cybersecurity is not solely dependent on technological solutions but also on structured education, user awareness, and behavioral factors.

Furthermore, the study identifies an imbalance in global research contributions and a relatively low level of international collaboration. These patterns suggest that the

development of cybersecurity education research is still concentrated in certain regions, potentially limiting the diversity and inclusiveness of perspectives within the field.

Suggestion

Based on the findings, several recommendations can be proposed. First, future research should further explore the integration of human-centered approaches, such as security awareness, behavioral change, and educational effectiveness, to complement existing technical perspectives in cybersecurity.

Second, there is a need to strengthen international collaboration among researchers, institutions, and countries. Increased cross-country partnerships can help promote knowledge exchange, enrich research diversity, and support the development of more inclusive and globally relevant cybersecurity education frameworks.

Third, policymakers and educators are encouraged to utilize these insights in designing and improving cybersecurity curricula, training programs, and awareness initiatives. Emphasis should be placed on aligning educational strategies with evolving cybersecurity challenges and user behavior.

Finally, future bibliometric studies may expand the scope of analysis by incorporating multiple databases or comparative approaches to provide a more comprehensive understanding of the field.

REFERENCE

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Ahmed, M., Kambam, H. R., Liu, Y., Jaidka, S., & Petrova, K. (2023). Impact and Significance of Human Factors in Digital Information Security. *International Journal of Information Science & Technology*. http://innove.org/ijist/

Ahmed Shan-A-Alahi. (2024). Cybersecurity Training and Its Influence on Employee Behavior in Business Environments. *Computer Fraud and Security*, 506–515. https://doi.org/10.52710/cfs.689

Al-Badayneh, D. M., Al-Badayneh, D. D., & Hashish, R. K. (2025). Human Factors of Cybersecurity. *Journal of Posthumanism*, *5*(4). https://doi.org/10.63332/joph.v5i4.1242

De Bruin, M., & Mersinas, K. (2022). *Individual and Contextual Variables of Cyber Security Behaviour*.

Fida Hasan, K., Hughes, W., & Rahman, A. (2025). *Gamifying Cyber Governance: A Virtual Escape Room to Transform Cybersecurity Policy Education*.

Kennison, S. M., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.546546

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3), 119. https://doi.org/10.1007/s10207-025-01032-0

Kumar, R. (2025). Bibliometric Analysis: Comprehensive Insights into Tools, Techniques, Applications, and Solutions for Research Excellence. *Spectrum of Engineering and Management Sciences*, *3*(1), 45–62. https://doi.org/10.31181/sems31202535k

Ngandu, M. R., Mwansa, G., & Mkabe, Z. (2025). Strengthening cybersecurity in a government department by addressing password management challenges and human factor vulnerabilities. *Discover Computing*, *28*(1), 148. https://doi.org/10.1007/s10791-025-09659-2

Oner, U., Cetin, O., & Savas, E. (2025). Human factors in phishing: Understanding susceptibility and resilience. *Computer Standards & Interfaces*, *94*, 104014. https://doi.org/10.1016/j.csi.2025.104014

Passas, I. (2024). Bibliometric Analysis: The Main Steps. *Encyclopedia*, *4*(2), 1014–1025. https://doi.org/10.3390/encyclopedia4020065

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, 103585. https://doi.org/10.1016/j.cose.2023.103585

Qureshi, R., & Koo, I. (2026). A Comprehensive Survey of Cybersecurity Threats and Data Privacy Issues in Healthcare Systems. *Applied Sciences*, *16*(3), 1511. https://doi.org/10.3390/app16031511

Sharma, D., Mittal, R., Sekhar, R., Shah, P., & Renz, M. (2023). A bibliometric analysis of cyber security and cyber forensics research. *Results in Control and Optimization*, *10*, 100204. https://doi.org/10.1016/j.rico.2023.100204

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, *119*, 102756. https://doi.org/10.1016/j.cose.2022.102756

Singh, P., Dutta, S., & Pranav, P. (2025). Network Security and Cryptography: Threats, Obstacles and Solutions - A Bibliometric Analysis. *Recent Advances in Computer Science and Communications*, *18*(2). https://doi.org/10.2174/0126662558280232231213053002

Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, & Samuel Onimisi Dawodu. (2024). CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY. *Computer Science & IT Research Journal*, *5*(1), 100–119. https://doi.org/10.51594/csitrj.v5i1.708

Verma, R., Gupta, N., & Kumar, A. (2025). A comprehensive scientometric study of research trends in cybersecurity from 2000 to 2024 using Biblioshiny and VOSviewer. *Discover Networks*, *1*(1). https://doi.org/10.1007/s44354-025-00011-0