West Science Interdisciplinary Studies
Vol. 03, No. 11, November and 2025: pp. 2059-2071

Bibliometric Analysis of Cybersecurity and Risk Management in Accounting

Loso Judijanto
IPOSS Jakarta, Indonesia and losojudijantobumn@gmail.com

ABSTRACT

This study performs a thorough bibliometric analysis to investigate the intellectual landscape and thematic evolution of cybersecurity and risk management research in the field of accounting. The study used Scopus-indexed articles and visual analytics produced via VOSviewer and Bibliometrix to delineate keyword co-occurrences, author collaborations, institutional networks, and contributions by countries. The findings indicate that cybersecurity, risk management, and risk assessment constitute the conceptual foundation of the discipline, acting as fundamental elements that link diverse related subjects such as network security, information management, cloud computing, blockchain, and data privacy. Temporal overlay analysis reveals a transition from an initial focus on technical vulnerabilities and fundamental risk assessment to a contemporary emphasis on digitalization, accounting system security, and developing technologies. Co-authorship and institutional networks exhibit fragmented yet expanding collaboration patterns, with the United States serving as the principal worldwide center. This study enhances the literature by delineating predominant topics, upcoming research frontiers, and collaboration deficiencies, so establishing a systematic basis for future investigations. These insights assist scholars and practitioners in formulating more cohesive, robust, and proactive cybersecurity measures inside accounting frameworks.

Keywords: *Cybersecurity, Risk Management, Accounting Information Systems, Bibliometric Analysis, Digitalization, Cyber Risk Assessment*

1. INTRODUCTION

The rapid digitalization of accounting processes has fundamentally altered the methods by which companies record, manage, store, and communicate financial data. Cloud-based accounting platforms, enterprise resource planning (ERP) systems, AI-driven analytics, and digital payment infrastructures have made it easier for businesses to improve efficiency, ensure real-time reporting, and make better decisions. However, these advancements also expose accounting systems to a new set of cybersecurity threats. Cyber-attacks, such as ransomware, phishing, unauthorized access, and tampering with digital financial records, pose a major threat to the privacy, accuracy, and availability of accounting data [1] [2]. As a result, cybersecurity has become an important part of how businesses manage risk as they use more technology in their accounting work.

Because digital corporate environments are so connected, accounting systems are even more open to cyber threats. Modern accounting information systems (AIS) are linked together by supply chains, e-commerce platforms, banks, and regulatory databases. This gives cybercriminals many ways to get in [3]. Companies that don't have strong internal controls or that still use old systems are more likely to be hacked, which can cost them money, slow down their operations, and hurt their reputation [4]. These worries show how important it is to understand how to use cybersecurity pr actices and risk management frameworks in accounting situations, as well as how important it is for scholars to study these issues.

In response to the growing number of cyber threats, regulatory bodies have created standards and guidelines for managing digital risks. Frameworks like COSO Enterprise Risk Management [5]. ISO/IEC 27001 [6] and cybersecurity guidelines from the American Institute of

Certified Public Accountants [7] show how important it is to include cyber risk factors in financial reporting and auditing. These developments underscore the necessity for accountants, auditors, and financial managers to attain expertise in digital security protocols as a fundamental component of their professional responsibilities.

Academic research in cybersecurity and accounting has significantly expanded but remains fragmented across various domains, including fraud detection [8] digital forensics [9]. audit analytics [10]. blockchain security [11] internal control systems [12] and privacy protection. The interdisciplinary nature of this field makes it harder to understand its conceptual framework and how its themes have changed over time. As a result, there is a growing need for a systematic approach to chart the development of academic discourse and identify current research trends.

Bibliometric analysis, including citation analysis, co-authorship networks, and keyword mapping, offers a thorough method for examining trends in scientific publications over time [13]. Bibliometrics can find important authors, important works, patterns of collaboration, and new themes through quantitative analysis. Given the increasing complexity of cyber-attacks—driven by artificial intelligence, state-sponsored actors, and the commercialization of compromised financial data—it is essential to understand how the academic community has conceptualized and responded to these challenges within the accounting discipline [14] This mapping is essential for theoretical advancement, policy development, and the enhancement of professional practice.

The importance of cybersecurity in accounting practices is increasing; however, the academic literature is fragmented and lacks a comprehensive synthesis that captures the evolution, framework, and thematic focus of research in this field. Prior studies focus on isolated topics—such as AIS vulnerabilities, cyber risk disclosure, audit analytics, or internal control deficiencies [15] [16] without incorporating them into a unified framework. This fragmentation makes it hard for researchers and practitioners to find important authors, intellectual clusters, common methodological approaches, and research gaps that are getting bigger. Thus, there is an immediate necessity for a bibliometric analysis that systematically outlines the progression of cybersecurity and risk management research in the domain of accounting.

This study aims to deliver a comprehensive bibliometric analysis of scholarly articles related to cybersecurity and risk management in the accounting domain. The goals are to (1) look into publication trends, well-known authors, important journals, and institutions that contribute; (2) look at citation frameworks and co-authorship networks to understand how ideas are connected and how people work together; (3) find co-occurring keywords, thematic clusters, and conceptual patterns to map out the intellectual landscape; (4) look at how research themes have changed over time; and (5) find gaps and suggest ways to improve cybersecurity and risk management research in accounting in the future. This study provides a comprehensive and evidence-based analysis, strengthening the theoretical framework, regulatory dialogue, and practical applications of cybersecurity in the accounting profession.

2. METHODS

This study employs a quantitative bibliometric methodology to analyze the evolution, structure, and intellectual landscape of research on cybersecurity and risk management in accounting. Bibliometric analysis enables the systematic assessment of large volumes of academic publications by analyzing citation patterns, co-authorship networks, keyword structures, and thematic clusters (Donthu et al., 2021). This scientific method conforms to established standards in science mapping and performance analysis (Aria & Cuccurullo, 2017). Data collection transpired in two phases: (1) procurement of scholarly publications and (2) structuring of obtained data for bibliometric visualization and statistical examination. To ensure relevance, the search method employed phrase combinations such as “cybersecurity,” “information security,” “cyber risk,” “risk management,” “accounting information systems,” “AIS security,” and “digital accounting.” These terms were employed in article titles, abstracts, and author-supplied keywords to enhance coverage and ensure the inclusion of relevant studies.

Data were sourced from the Scopus database, chosen for its comprehensive indexing of peer-reviewed papers, wide-ranging disciplinary coverage, and suitability for bibliometric analysis [17]The search included all papers available until early 2025 to determine historical and contempor ary trends. Only articles, conference papers, and review papers published in English were retained to ensure consistency and scholarly integrity. Exclusions were applied to things such as book chapters, editorials, letters, and non-scholarly articles. The acquired documents were meticulously scrutinized to remove duplicates and other materials unrelated to accounting or cybersecurity. The final dataset was generated in CSV and RIS formats for analytical purposes. Descriptive bibliometric characteristics, including publication growth, citation distributions, leading authors, contributing institutions, and prominent journals, were computed to provide an overview of the research landscape and its academic impact.

Advanced bibliometric mapping techniques were utilized through VOSviewer ([18] and the Bibliometrix package in R [19] Co-authorship analysis revealed collaboration networks and leading research groups in the field, while co-citation analysis clarified the intellectual foundations of cybersecurity and risk management research in accounting. Keyword co-occurrence mapping clarified dominant conceptual themes and emerging research domains. Strategic diagrams and thematic evolution maps generated with Biblioshiny provided insights into the chronological advancement of the discipline, emphasizing shifts in research aims and the evolution of specific topics. The study utilizes diverse bibliometric techniques to deliver a comprehensive and nuanced understanding of the conceptualization, evolution, and interconnection of cybersecurity and risk management throughout accounting literature.

3. RESULTS AND DISCUSSION

3.1 Network Visualization

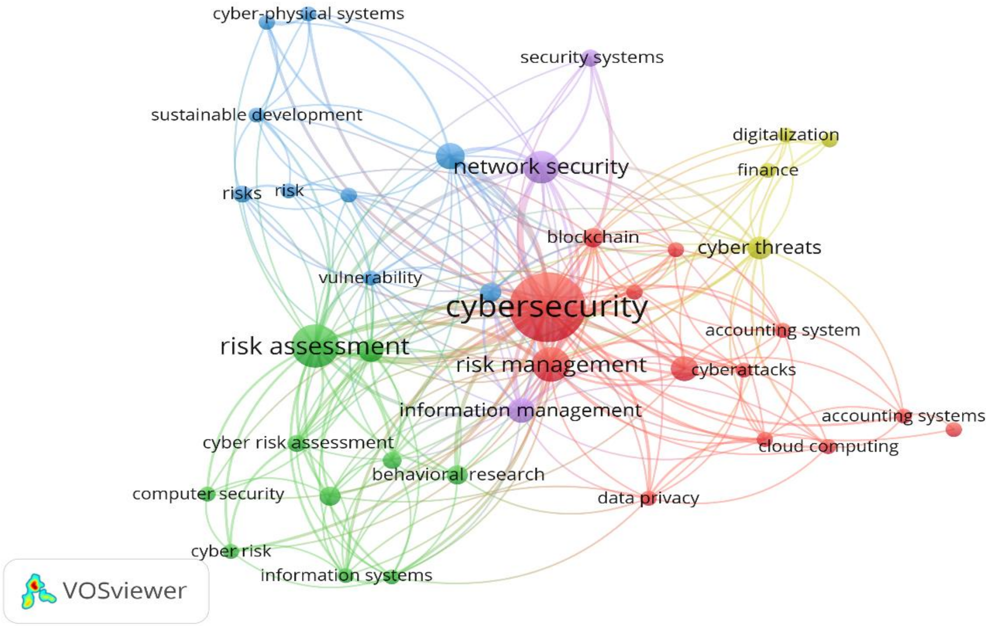

Figure 1. Network Visualization

Source: Data Analysis Result, 2025

The VOSviewer map depicts that cybersecurity is the predominant and most central keyword, as seen by its greatest node size and high connection density. This location signifies its function as the intellectual nucleus of the research domain, interlinking several theme areas such as network security, risk assessment, cyber threats, accounting systems, cloud computing, and data privacy. The concentrated focus on "cybersecurity" indicates that accounting research is progressively including cybersecurity factors into its evaluations of risk, information management, and technology adoption. The network demonstrates that cybersecurity research is multidisciplinary, integrating concepts from computer science, information systems, behavioral studies, and accounting.

A significant topic cluster (green) focuses on risk assessment and its derivatives, including "cyber risk assessment," "risk," "risks," and "computer security." This cluster delineates the methodological and analytical underpinnings of cybersecurity research, highlighting frameworks employed to detect, quantify, and assess vulnerabilities in organizational systems. The closeness of terms such as "vulnerability," "behavioral research," and "information systems" indicates that risk assessment research encompasses both technical and human aspects of cyber risk, emphasizing the significance of employee conduct, internal controls, and system architecture in mitigating cyber incidents. This accords with modern study that emphasizes socio-technical perspectives on cyber risk in digital accounting contexts.

A distinct cluster (blue and purple) pertains to network security and security systems, signifying the more technical contributions to the domain. Terms like "cyber-physical systems," "sustainable development," and "security systems" suggest that researchers are investigating the impact of interconnected infrastructures and sophisticated digital ecosystems on organizational vulnerability to cyber threats. The relationship between cyber-physical systems and cybersecurity indicates a broadening of accounting-related cybersecurity research into domains where digital financial systems converge with operational technology, highlighting the increasing necessity for cyber safeguards in integrated business settings.

The red and yellow clusters emphasize subjects closely associated with accounting and business operations, such as "accounting systems," "accounting system," "cloud computing," "data privacy," "digitalization," and "finance." These terms illustrate the impact of cybersecurity risks on fundamental accounting functions, including the integrity of financial data, the reliability of cloud-based accounting systems, and the confidentiality of critical organizational information. The occurrence of "blockchain" in the center region signifies increasing interest in distributed ledger technology as both a prospective remedy and a potential weakness. The proximity of phrases such as "cyberattacks," "cyber threats," and "cyber risk" to accounting-related terminology indicates an increasing acknowledgment that financial data infrastructures are primary targets for cybercrime, hence enhancing the significance of cybersecurity governance in accounting.

The distribution of clusters and the robustness of cross-connections indicate a developing study domain with progressively integrated viewpoints. The intersecting color lines indicate that cybersecurity and risk management in accounting are now integrated elements of a wider discourse on digitalization and risk governance. Research involves associating risk assessment methodologies with developing technologies, amalgamating behavioral viewpoints with technical safeguards, and correlating conventional accounting systems with modern cybersecurity frameworks. The network visualization illustrates a dynamic intellectual landscape marked by convergence, multidisciplinary collaboration, and shifting topic emphasis, highlighting the complexity and strategic significance of cybersecurity research within the accounting discipline.

3.2 Overlay Visualization

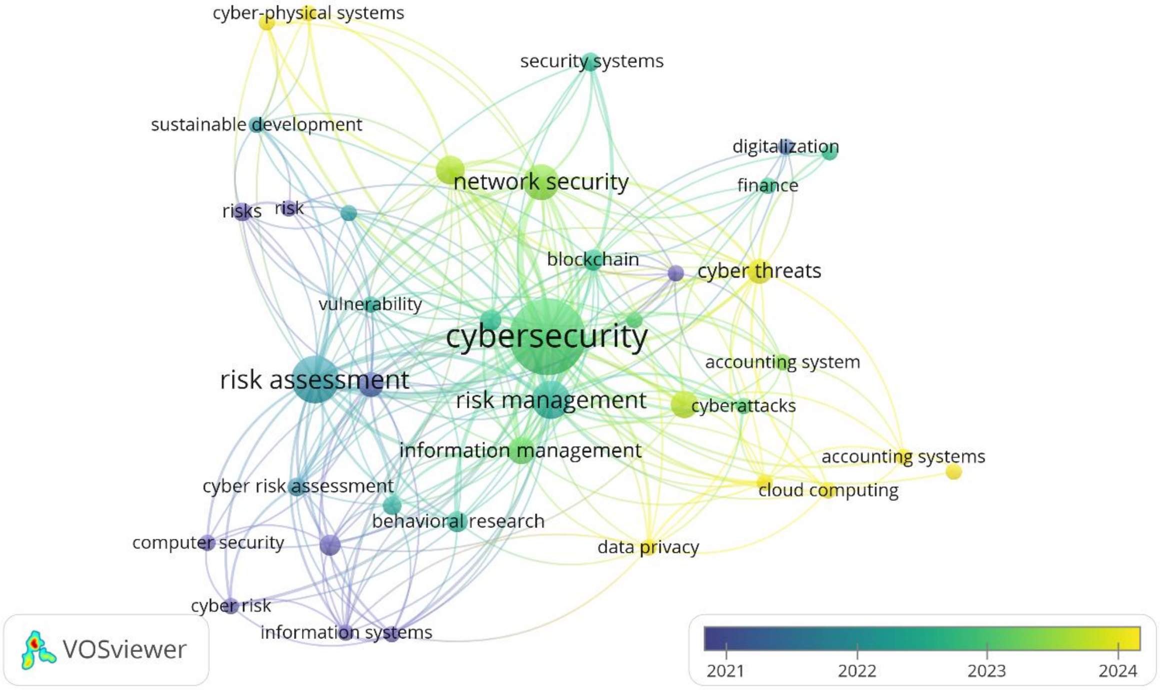

Figure 2. Overlay Visualization
Source: Data Analysis Result, 2025

The overlay visualization demonstrates a temporal progression in the research landscape, emphasizing the shift in academic focus from 2021 to 2024. Previous studies—illustrated in deeper blue—primarily focused on fundamental principles including risk assessment, computer security, information systems, vulnerabilities, and cyber risk evaluation. These themes illustrate the field's primary emphasis on comprehending technical vulnerabilities, assessing systemic threats, and developing methodological risk assessment frameworks. In this earlier phase, research primarily focused on delineating the characteristics of cyber hazards and formulating fundamental security measures for digital accounting settings.

As the timeline advances toward 2022–2023 (green shades), the network demonstrates a diversification of research interests, indicating the incorporation of cybersecurity into wider dimensions of organizational governance and technological implementation. Developing associations concerning terms like network security, risk management, information management, and behavioral research suggest a transition towards socio-technical viewpoints. This mid-period demonstrates heightened focus on blockchain, data privacy, and security technologies, indicating escalating apprehension regarding the protection of financial data amidst swift digital development. The domain increasingly investigates the interplay between sophisticated technology, distributed ledgers, and organizational controls in shaping cybersecurity capabilities inside accounting systems.

The yellow nodes, symbolizing late-emerging themes (2023–2024), demonstrate a current shift towards digital integration and application-level risks in accounting. Terminology such as cloud computing, cyber risks, cyberattacks, accounting systems, digitization, and finance is at the forefront of contemporary research endeavors. This indicates an increased awareness of risks in cloud-based accounting systems and digitally interconnected financial frameworks. The connection between cybersecurity and accounting-specific elements signifies a more advanced stage of research, wherein cybersecurity is regarded not merely as a technical concern but as an essential aspect of financial integrity, audit dependability, and organizational risk management. The overlay graphic collectively illustrates a progression from fundamental risk assessment to modern research focused on real-time cyber threats, digital transformation, and vulnerabilities in accounting systems.

3.3 Citation Analysis

To comprehend the intellectual underpinnings and thematic progression of cybersecurity and risk management in accounting, it is crucial to identify the most significant publications that have influenced the discourse in this domain. Prominently referenced studies provide essential in sights into critical research priorities, methodological innovations, and conceptual frameworks that direct modern scholarship. The subsequent table encapsulates the most referenced publications within the dataset, emphasizing their contributions to cybersecurity, accounting systems, risk governance, and interdisciplinary connections across information systems, behavioral science, and operations management. These significant studies illustrate the extensive scope of research and e mphasize the critical role of cybersecurity in accounting and organizational decision-making.

Table 1. The Most Impactful Literatures

Citations	Authors and year	Title
77	Walton, S., Wheeler, P.R., Zhang, Y., Zhao, X. (2021)	An integrative review and analysis of cybersecurity research current state and future directions
66	Haapamäki, E., Sihvonen, J. (2019)	Cybersecurity in accounting research
61	Neigel, A.R., Claypoole, V.L., Waldfogle, G.E., Acharya, S., Hancock, G.M. (2020)	Holistic cyber hygiene education: Accounting for the human factors
56	Sardi, A., Rizzi, A., Sorano, E., Guerrieri, A. (2020)	Cyber risk in health facilities: A systematic literature review
53	Rodger, J.A., George, J.A. (2017)	Triple bottom line accounting for optimizing natural gas sustainability: A statistical linear programming fuzzy ILOWA optimized sustainment model approach to reducing supply chain global cybersecurity vulnerability through information and communications technology
51	Scala, N.M., Reilly, A.C., Goethals, P.L., Cukier, M. (2019)	Risk and the Five Hard Problems of Cybersecurity
46	Bodin, L.D., Gordon, L.A., Loeb, M.P., Wang, A. (2018)	Cybersecurity insurance and risk-sharing
39	Naffa, H., Fain, M. (2020)	Performance measurement of ESG-themed megatrend investments in global equity markets using pure factor portfolios methodology
32	Paul, J.A., Zhang, M. (2021)	Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker
31	Eaton, T.V., Grenier, J.H.,	Accounting and cybersecurity risk management

Citations	Authors and year	Title
	Layman, D. (2019)	

Source: Scopus, 2025

The table underscores a varied yet interrelated corpus of significant research that collectively shapes the contemporary comprehension of cybersecurity in accounting. [20] and [21] offer basic analyses that delineate significant trends and position cybersecurity as a burgeoning field within accounting research. Research by [22] and [23] underscores the essential influence of human behavior and cognitive elements in mitigating cyber risk, indicating that technology protections are inadequate without a supportive company culture and heightened employee awareness. Simultaneously, the studies by [24] and [25] highlight the increasing significance of economic modeling, insurance strategies, and decision-support systems in the management of cyber risks at both corporate and governmental tiers. Numerous studies expand the conversation on cybersecurity beyond conventional accounting limits. [26] integrate cybersecurity with sustainability and supply chain risk, demonstrating the complex risks inherent in digital infrastructures. [27] illustrate the ubiquity of cyber hazards in healthcare settings, highlighting the cross-sectoral importance of cybersecurity. [28] establish a direct connection between cybersecurity risk management and accounting procedures, emphasizing the necessity of incorporating cyber governance into financial reporting, auditing, and corporate risk management frameworks. Collectively, these extensively referenced studies illustrate a developing research environment marked by interdisciplinary methodologies, enhanced methodological complexity, and an escalating acknowledgment of cybersecurity as a pivotal element of accounting and organizational risk management.

3.4 Density Visualization

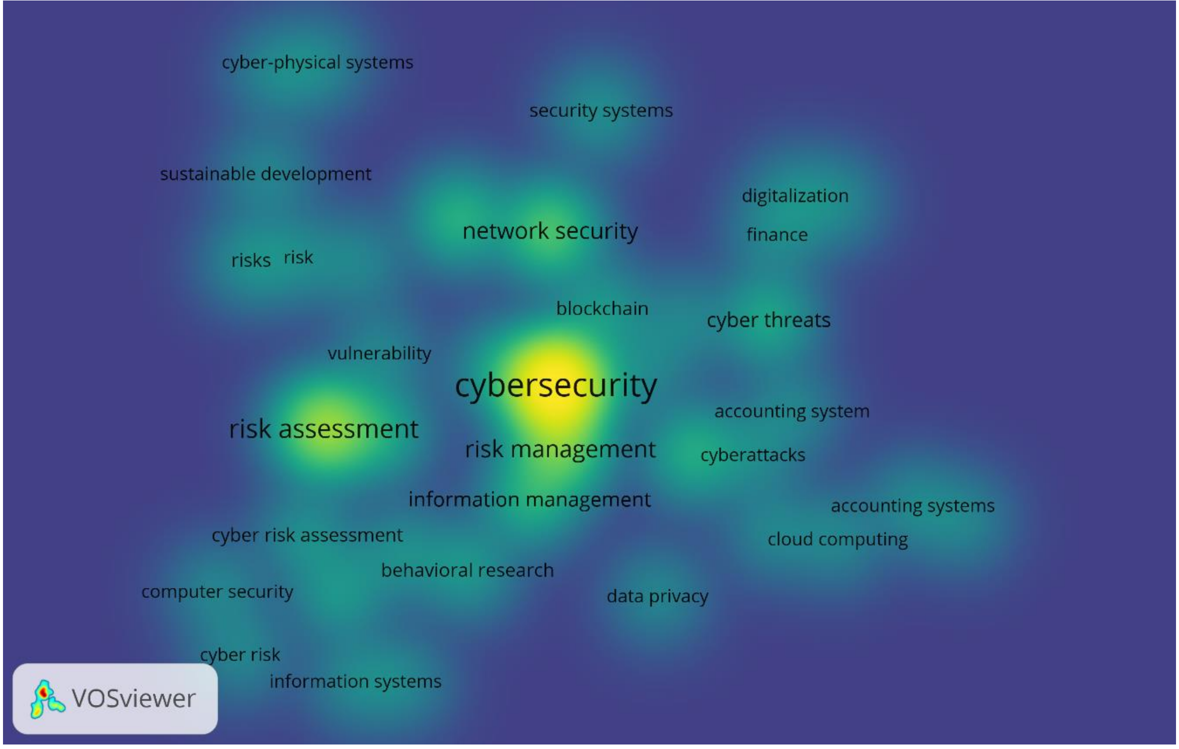

Figure 3. Density Visualization

Source: Data Analysis Result, 2025

The density depiction underscores cybersecurity as the predominant and most impactful theme in the research landscape, indicated by the bright yellow area at the center of the map. This signifies that cybersecurity is the predominant keyword and serves as the conceptual foundation for related issues such as risk management, risk assessment, information management, and network security. The neighboring themes are represented in lighter green patches, indicating a high yet relatively lower density, implying that they are significant but subordinate to the primary cybersecurity debate. The aggregation of pertinent terms such as vulnerability, cyber risk assessment, and computer security around these central themes demonstrates a significant concentration of research aimed at threat evaluation, risk assessment, and the development of system-level protective measures—aligning with the field's technical and analytical emphasis.

The peripheral yet discernible green zones surrounding phrases such as cloud computing, accounting systems, data privacy, and cyberattacks signify burgeoning areas of specialty attracting heightened scholarly interest. Their positioning on the periphery of the high-density core indicates that these issues are gaining traction but have not yet attained the central influence of more established structures. The emergence of blockchain, digitalization, and finance in mid-density areas indicates an increasing incorporation of cybersecurity issues into digital accounting and financial technologies. The density map indicates a research domain centered on cybersecurity and risk assessment, with increasing interest in applied areas such as cloud-based accounting, cyber-physical systems, and privacy protection—indicating a transition towards wider, multidisciplinary involvement in cybersecurity within accounting frameworks.

3.5 Co-Authorship Network

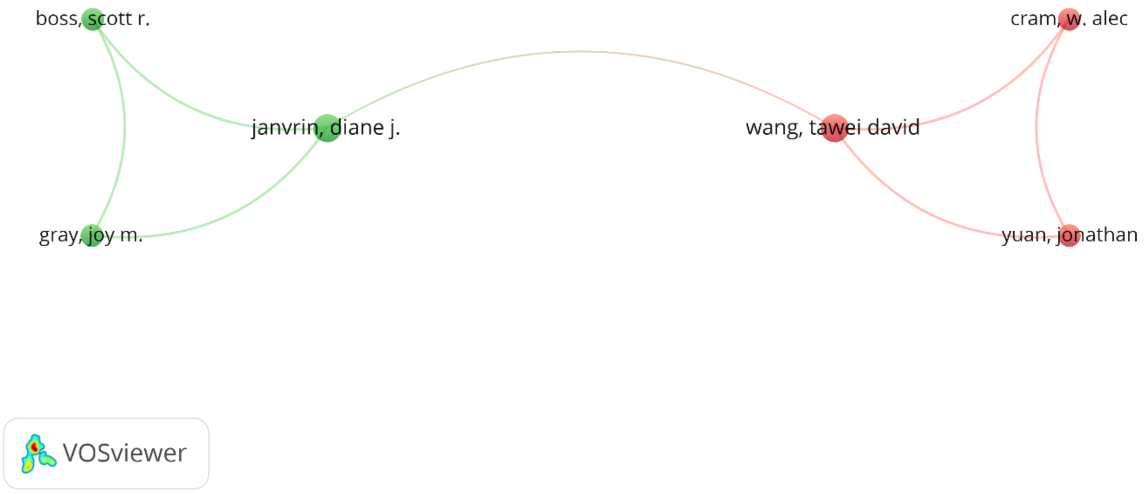

Figure 4. Author Visualization

Source: Data Analysis Result, 2025

The VOSviewer co-authorship among writers indicates two separate clusters of collaboration in the fields of cybersecurity and accounting research. The initial cluster includes Diane J. Janvrin, Scott R. Boss, and Joy M. Gray, whose robust links suggest regular collaborative publications and common research interests, presumably focused on the behavioral and organizational dimensions of cybersecurity in accounting settings. The second cluster comprises Tawei David Wang, W. Alec Cram, and Jonathan Yuan, who collaborate on subjects pertaining to information systems security, cyber risk governance, and accounting analytics. The tenuous connection between Janvrin and Wang indicates sporadic cross-cluster collaboration, suggesting that although there are cohesive research teams within the area, overall author collaboration is restricted and somewhat disjointed. This framework emphasizes prospects for future interdisciplinary collaborations that may enhance theoretical integration and broaden the scope of cybersecurity research within accounting.

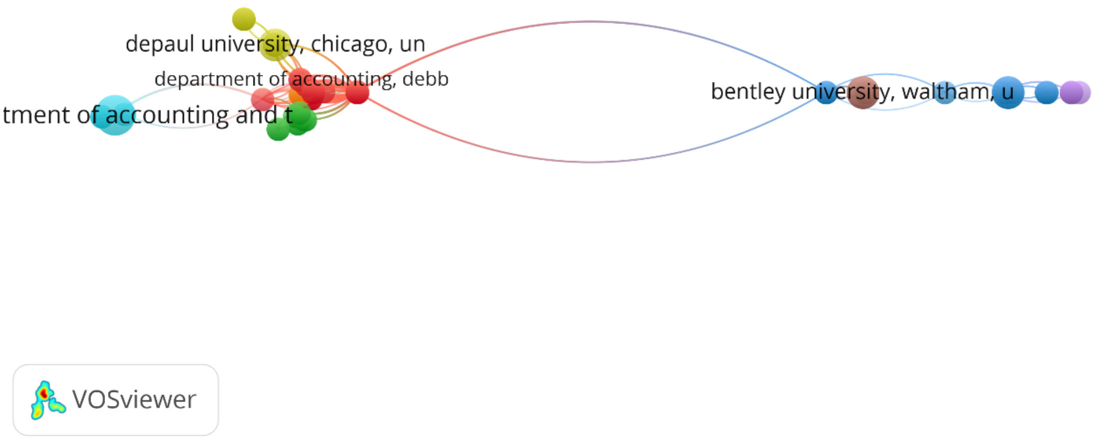
depaul university, chicago, un
department of accounting, debb
tment of accounting and t
bentley university, waltham, u
VOSviewer

Figure 5. Affiliation Visualization
Source: Data Analysis Result, 2025

The visualization of institutional collaboration reveals two predominant clusters that lead research endeavors in cybersecurity and accounting. The initial cluster, centered around entities like DePaul University and various accounting departments represented by green and yellow nodes, illustrates a robust internal collaboration network, signifying that these institutions often co-author research or engage in intersecting research groups. The second cluster, represented by Bentley University and its affiliated departments, constitutes a similarly integrated research powerhouse on the other side of the map. The restricted bridging relationship between these two prominent clusters indicates that although both institutional groups actively contribute to the subject, collaborative research across institutions is still rather infrequent. This fragmentation indicates that cybersecurity research in accounting is predominantly propelled by institution-specific initiatives rather than extensive inter-university collaborations, underscoring considerable opportunities for enhancing cross-institutional cooperation to bolster knowledge integration and research efficacy.

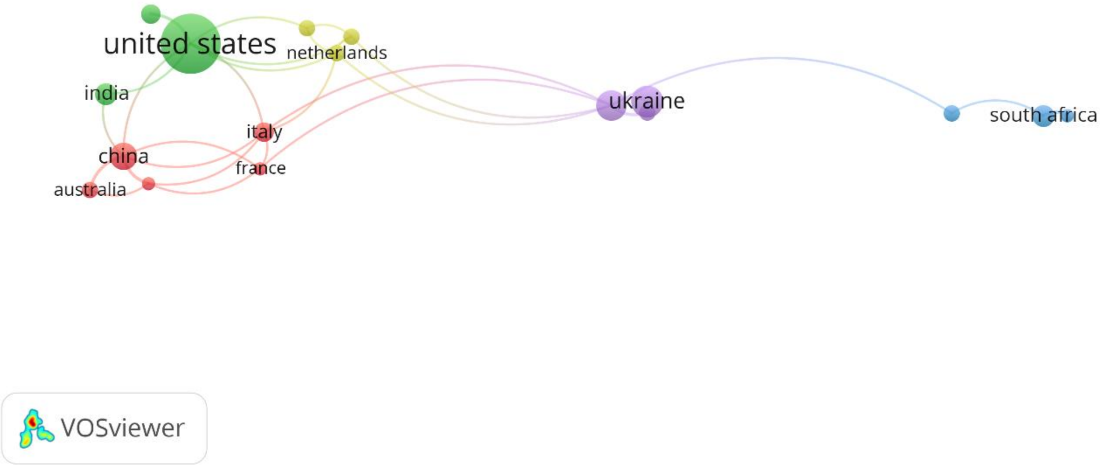

Figure 6. Country Visualization
Source: Data Analysis Result, 2025

The VOSviewer co-country of international collaboration illustrates the United States as the preeminent provider to cybersecurity and accounting research, as seen by its substantial node size and extensive collaboration ties with nations such China, India, the Netherlands, Italy, France, and Australia. This key position indicates that the U.S. functions as a principal nexus for global research collaborations, facilitating transnational knowledge transfer on cyber risk, digital security, and accounting systems. European nations, such as the Netherlands, Italy, and France, exhibit interlinked research endeavors, establishing a secondary collaborative network in conjunction with contributions from China and India. Simultaneously, Ukraine and South Africa emerge as peripheral nodes, signifying nascent yet constrained involvement in global research collaborations. The map indicates a field predominantly centered in Western and Asian research hubs, with significant potential for enhancing international collaborations to bolster global comprehension of cybersecurity issues in accounting.

Discussions

Practical Implications

This study's conclusions provide several practical consequences for companies, policymakers, and accounting professionals. The paramount importance of cybersecurity, risk assessment, and network security highlights the necessity for companies to enhance cyber governance as a fundamental component of their accounting framework. Organizations may leverage these insights to prioritize investments in secure accounting systems, enhance cloud-based data protection, and establish complete cyber risk assessment frameworks in accordance with global standards like as ISO 27001 and COSO ERM. The recognition of developing subjects—such as cloud computing, blockchain, data privacy, and digitalization—indicates that professionals must augment their abilities beyond conventional accounting to encompass digital literacy and in formation security awareness. The disjointed engagement patterns among institutions and nations highlight the necessity for enhanced cross-sector and international partnerships to exchange best practices, mitigate cybersecurity vulnerabilities, and strengthen global resilience in financial reporting systems. The paper provides a framework for synchronizing accounting practices with the swiftly changing cybersecurity environment.

Theoretical Contribution

This study conceptually contributes by delineating the intellectual framework of cybersecurity and risk management within the accounting field, providing a greater comprehension of the evolution and interconnection of research issues across time. The study identifies fundamental theoretical domains through the analysis of keyword co-occurrence, co-authorship, and institutional networks, including socio-technical perspectives on cyber risk, behavioral theories of security compliance, and risk management frameworks that encompass both technological and human elements. The bibliometric approach also uncovers conceptual deficiencies, such the inadequate integration of cybersecurity theories with accounting information system models and the insufficient development of frameworks linking digitalization, ESG considerations, and cyber risk governance. Moreover, the interdisciplinary character of significant articles underscores the theoretical alignment of information systems research, behavioral science, and accounting, providing scholars with a basis for formulating more comprehensive cyber risk theories. This study enhances the theoretical framework by elucidating prevailing paradigms and proposing new directions for future research advancement.

Limitations

This work, despite its contributions, has numerous shortcomings that require acknowledgment. The analysis predominantly utilizes the Scopus database, which, while extensive, may omit pertinent publications indexed in Web of Science, IEEE Xplore, or industry-specific ar chives, hence potentially constraining the dataset's scope. Secondly, bibliometric tools identify structural patterns and publication trends; nevertheless, they do not evaluate the qualitative depth of theoretical arguments, methodological rigor, or the practical impact of particular research. Cons equently, interpretations are contingent upon publication frequency and citation metrics, potentia lly privileging older or more readily accessible publications. Third, the co-authorship and country networks reveal collaborative tendencies but fail to comprehensively elucidate contextual factors—such as funding availability, regional cybersecurity regulations, or institutional research priorities—that influence these patterns. The swiftly advancing landscape of cybersecurity indicates that new threats, technology, and legislative modifications may surpass the publication cycle, resulting in a temporal discrepancy between actual developments and scholarly perspectives. Subsequent research may rectify these limitations by using mixed-method approaches, broadening multi-database coverage, and performing more comprehensive thematic or content analysis.

CONCLUSION

This bibliometric analysis offers a thorough delineation of the intellectual framework, thematic progression, and collaborative networks in the domain of cybersecurity and risk management in accounting. The findings indicate that cybersecurity has become the principal and unifying topic linking diverse study areas, such as risk assessment, network security, information management, cloud computing, and accounting information systems. The dense focus on terms like cybersecurity, risk management, and risk assessment underscores the importance of these concepts in modern accounting research, highlighting an increasing acknowledgment of cyber threats as significant organizational risks that necessitate strong governance frameworks. The data reveals substantial changes in research priorities over time. Initial research focused on technical vulnerabilities, cybersecurity, and fundamental risk assessment frameworks. Conversely, recent research have broadened to encompass digital transformation subjects including cloud-based accounting, blockchain technology, data privacy, and cyber-physical systems. This transition indicates the discipline's adjustment to more intricate digital landscapes, where accounting systems are intricately integrated inside extensive organizational information frameworks. The rise of behavioral research themes indicates that cybersecurity in accounting is now perceived not only from a technological perspective but also in relation to human aspects, decision-making processes, and corporate culture. Collaboration patterns indicate a domain characterized by expanding yet still disjointed networks. Author-level clusters reveal areas of robust collaboration with restricted inter group connectivity, whereas institutional and country-based networks show that the United States continues to be the central center of worldwide academic activity. The involvement of nations like China, India, the Netherlands, Italy, Ukraine, and South Africa signifies a growing global interest in cyber risk matters, fostering prospects for varied and interdisciplinary collaborations. Fortifying these international connections could expedite theoretical advancement and augment the practical significance of cybersecurity research in accounting. This study enhances the literature by providing a systematic assessment of the field's past and future directions. It delineates main research clusters, nascent issues, and collaborative deficiencies, establishing a basis for scholars, practitioners, and policymakers aiming to improve cybersecurity governance within accounting frameworks. With the rapid advancement of digitalization and the evolution of cyber risks, ongoing research is crucial to maintaining the resilience, integrity, and efficacy of accounting systems in facilitating sound financial decision-making within a more interconnected environment.

REFERENCES

[1] H. Liang, Y. Xue, A. Pinsonneault, and Y. “Andy” Wu, “What Users Do besides Problem-Focused Coping When Facing IT Security Threats,” *MIS Q.*, vol. 43, no. 2, pp. 373-A18, 2019.

[2] D. Dang-Pham and S. Pittayachawan, “Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach,” *Comput. Secur.*, vol. 48, pp. 281–297, 2015.

[3] Y. A. Jasim and M. B. Raewf, “Impact of the information technology on the accounting system,” *Cihan Univ. J. Humanit. Soc. Sci.*, vol. 4, no. 1, pp. 50–57, 2020.

[4] G. Kruss, I. Petersen, M. Sanni, D. Adeyeye, and A. Egbetokun, “Do we measure what should be measured? Towards a research and theoretical agenda for STI measurement in Africa,” *Innov. Dev.*, pp. 1–25, 2025.

[5] L. L. P. PricewaterhouseCoopers, “Committee of Sponsoring Organizations of the Treadway Commission (COSO).(2017) Enterprise Risk Management: Integrating with Strategy and Performance,” *New York COSO*, pp. 69–74.

[6] D. Ganji, C. Kalloniatis, H. Mouratidis, and S. M. Gheytassi, “Approaches to develop and implement iso/iec 27001 standard-information security management systems: A systematic literature review,” *Int. J. Adv. Softw*, vol. 12, no. 3, 2019.

[7] AICPA, *Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2017*. John Wiley & Sons, 2017.

[8] K. M. Zakaria, A. Nawawi, and A. S. A. P. Salin, “Internal controls and fraud–empirical evidence from oil and gas company,” *J. Financ. crime*, vol. 23, no. 4, pp. 1154–1168, 2016.

[9] H. Carvey and C. Altheide, *Digital forensics with open source tools*. Elsevier, 2011.

[10] M. A. Vasarhelyi, A. Kogan, and B. M. Tuttle, “Big data in accounting: An overview,” *Account. Horizons*, vol. 29, no. 2, pp. 381–396, 2015.

[11] D. Yermack, “Corporate governance and blockchains,” *Rev. Financ.*, vol. 21, no. 1, pp. 7–31, 2017.

[12] C. Liu and M. A. Babar, “Corporate cybersecurity risk and data breaches: A systematic review of empirical research,” *Aust. J. Manag.*, p. 03128962241293658, 2024.

[13] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, “How to conduct a bibliometric analysis: An overview and guidelines,” *J. Bus. Res.*, vol. 133, pp. 285–296, 2021.

[14] S. Masmoudi, “Unveiling the human factor in cybercrime and cybersecurity: Motivations, behaviors, vulnerabilities, mitigation strategies, and research methods,” in *Cybercrime unveiled: Technologies for analysing legal complexity*, Springer, 2025, pp. 41–91.

[15] W. Chen, H. Ren, and Z. Huang, “Does carbon emission trading system facilitate corporate digital transformation? Evidence from China,” *Total Qual. Manag. Bus. Excell.*, vol. 36, no. 11–12, pp. 1301–1329, 2025.

[16] G. Tan, “Uncovering Role of Information Security Awareness, Compliance Knowledge & Organizational Citizenship Behaviour Towards Information Security Compliance in Chinese Public & Private Universities,” *Prof. la Inf.*, vol. 33, no. 5, 2024.

[17] P. Mongeon and A. Paul-Hus, “The journal coverage of Web of Science and Scopus: a comparative analysis,” *Scientometrics*, vol. 106, no. 1, pp. 213–228, 2016.

[18] N. Van Eck and L. Waltman, “Software survey: VOSviewer, a computer program for bibliometric mapping,” *Scientometrics*, vol. 84, no. 2, pp. 523–538, 2010.

[19] M. Aria and C. Cuccurullo, “bibliometrix: An R-tool for comprehensive science mapping analysis,” *J. Informetr.*, vol.

11, no. 4, pp. 959–975, 2017.

[20] S. Walton, P. R. Wheeler, Y. Zhang, and X. Zhao, "An integrative review and analysis of cybersecurity research: Current state and future directions," *J. Inf. Syst.*, vol. 35, no. 1, pp. 155–186, 2021.

[21] E. Haapamäki and J. Sihvonen, "Cybersecurity in accounting research," *Manag. Audit. J.*, vol. 34, no. 7, pp. 808–834, 2019.

[22] A. R. Neigel, V. L. Claypoole, G. E. Waldfogle, S. Acharya, and G. M. Hancock, "Holistic cyber hygiene education: Accounting for the human factors," *Comput. Secur.*, vol. 92, p. 101731, 2020.

[23] N. M. Scala, A. C. Reilly, P. L. Goethals, and M. Cukier, "Risk and the five hard problems of cybersecurity," *Risk Anal.*, vol. 39, no. 10, pp. 2119–2126, 2019.

[24] L. D. Bodin, L. A. Gordon, M. P. Loeb, and A. Wang, "Cybersecurity insurance and risk-sharing," *J. Account. Public Policy*, vol. 37, no. 6, pp. 527–544, 2018.

[25] J. A. Paul and M. Zhang, "Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker," *Eur. J. Oper. Res.*, vol. 291, no. 1, pp. 349–364, 2021.

[26] J. A. Rodger and J. A. George, "Triple bottom line accounting for optimizing natural gas sustainability: A statistical linear programming fuzzy ILOWA optimized sustainment model approach to reducing supply chain global cybersecurity vulnerability through information and communications technology," *J. Clean. Prod.*, vol. 142, pp. 1931–1949, 2017.

[27] A. Sardi, A. Rizzi, E. Sorano, and A. Guerrieri, "Cyber risk in health facilities: A systematic literature review," *Sustainability*, vol. 12, no. 17, p. 7002, 2020.

[28] T. V Eaton, J. H. Grenier, and D. Layman, "Accounting and cybersecurity risk management," *Curr. Issues Audit.*, vol. 13, no. 2, pp. C1–C9, 2019.