http://dx.doi.org/10.18623/rvd.v22.n7.3815

CYBERSECURITY IN FINANCIAL INSTITUTIONS: A BIBLIOMETRIC AND THEMATIC ANALYSIS OF GLOBAL RESEARCH (2000–2025)

CIBERSEGURANÇA EM INSTITUIÇÕES FINANCEIRAS: UMA ANÁLISE BIBLIOMÉTRICA E TEMÁTICA DA PESQUISA GLOBAL (2000–2025)

Article received on: 8/15/2025
Article accepted on: 11/14/2025

Marek Pekarčík*
*Technical University of Košice, Faculty of Economics, Department of Economics, Němcovej, Košice, Slovakia,
Orcid: https://orcid.org/0000-0002-1384-4304
marek.pekarcik@tuke.sk

Jakub Sopko*
*Technical University of Košice, Faculty of Economics, Department of Banking and Investment, Němcovej, Košice, Slovakia,
Orcid: https://orcid.org/0000-0002-7314-828X
jakub.sopko@tuke.sk

Leoš Šafár*
*Technical University of Košice, Faculty of Economics, Department of Banking and Investment, Němcovej, Košice, Slovakia,
Orcid: https://orcid.org/0000-0001-8466-0644
leos.safar@tuke.sk
(Corresponding author)

The authors declare that there is no conflict of interest

Abstract
Cybersecurity has become a central element of operational risk in the financial sector, where rapid digitalization and increasingly interconnected technologies expose institutions to sophisticated cyber threats. This study offers a bibliometric and content-based analysis of cybersecurity research in banking and insurance, drawing on 2,005 publications indexed in the Web of Science (2000–2025) and analyzed using the Bibliometrix R package. The findings show steady growth in research output, driven by regulatory developments, technological innovation, and the expansion of digital financial services. The literature remains highly dispersed, with limited source concentration and uneven patterns of international collaboration: high-output countries such as the United States and India exhibit comparatively low collaboration ratios, whereas smaller contributors, including Saudi Arabia and Australia, show stronger global integration. Thematic clusters reveal three principal research fronts: AI-enabled threat detection, institutional cybersecurity governance, and fintech-related security issues. Despite this expansion, empirical gaps persist, particularly regarding the effectiveness of cybersecurity investments and the limited

Resumo
A cibersegurança tornou-se um componente central do risco operacional no setor financeiro, onde a rápida digitalização e a crescente interconectividade tecnológica expõem as instituições a ameaças cibernéticas cada vez mais sofisticadas. Este estudo apresenta uma análise bibliométrica e de conteúdo da pesquisa em cibersegurança aplicada aos setores bancário e segurador, com base em 2.005 publicações indexadas na Web of Science (2000–2025) e analisadas por meio do pacote Bibliometrix em R. Os resultados indicam crescimento contínuo da produção científica, impulsionado por avanços regulatórios, inovação tecnológica e expansão dos serviços financeiros digitais. A literatura mostra elevada dispersão, com pouca concentração de periódicos e padrões desiguais de colaboração internacional: países com alta produção, como Estados Unidos e Índia, apresentam baixa intensidade colaborativa, enquanto contribuintes menores, como Arábia Saudita e Austrália, demonstram maior integração global. A análise temática identifica três frentes principais: detecção de ameaças com apoio de IA, governança institucional da cibersegurança e questões de segurança relacionadas a fintechs.

attention given to the insurance sector. The study's reliance on English-language WoS data and bibliometric methods represents a key limitation. Overall, the results highlight cybersecurity as a strategic priority for financial systems and underscore the need for more interdisciplinary, empirically grounded, and internationally coordinated research.

Keywords: Cybersecurity. Fintech. Bibliometric Analysis. Financial Institutions.

Persistem lacunas empíricas relevantes, especialmente quanto à efetividade dos investimentos em cibersegurança e à pouca atenção dedicada ao setor de seguros. Os achados reforçam a cibersegurança como prioridade estratégica e destacam a necessidade de pesquisas mais interdisciplinares, empíricas e coordenadas internacionalmente.

Palavras-chave: *Cibersegurança. Fintech. Análise Bibliométrica. Instituições Financeiras.*

1 INTRODUCTION

Digital transformation has profoundly reshaped the financial sector over the past two decades, making financial institutions increasingly dependent on interconnected information systems for the delivery of essential services. While this technological evolution has improved efficiency, accessibility, and market integration, it has simultaneously intensified exposure to sophisticated cyber risks (Darem et al., 2023). Cyberattacks now affect financial institutions with greater frequency and complexity, posing threats not only to individual entities but also to systemic financial stability (Al-Alawi & Al-Bassam, 2020; Alzoubi et al., 2022). The IMF estimates that cyber incidents may erode nearly 9% of global banking profits, underscoring the scale of this challenge (Bouveret, 2018).

The concept of cyber risk remains difficult to define due to its interdisciplinary nature and the diversity of its causes and consequences (Kaffenberger & Kopp, 2019). It spans fields such as information technology, information security, finance, economics, and organizational studies (Matejka et al., 2021; Sheehan et al., 2021). For analytical purposes, cyber risk is commonly understood as a form of operational risk associated with disruptions to information and technology assets that threaten the confidentiality, integrity, or availability of systems (Pacelli, 2025).

Despite increasing awareness, scholarly work on cybersecurity in financial institutions remains dispersed across technical, economic, regulatory, and managerial domains. Empirical, sector-specific research (particularly focused on banking and insurance) continues to lag behind conceptual and policy-oriented discussions. Regulatory bodies including the Basel Committee, the IMF, and the OECD have

repeatedly emphasized the need to integrate cybersecurity more systematically into financial supervision and risk management frameworks.

As noted by Barcellos-Paula et al. (2025), the absence of dedicated bibliometric studies limits our understanding of how research on cybersecurity in the financial sector has evolved, which themes dominate the field, and where emerging gaps lie. This study responds to that need by providing a bibliometric and content-driven analysis of cybersecurity scholarship within financial institutions. Drawing on data from the Web of Science and analysed using the Bibliometrix R package, it maps key publications, authors, concepts, and collaborative patterns from 2000 to June 2025.

By consolidating the fragmented academic landscape, this study offers a structured overview of the intellectual development of cybersecurity research in finance and contributes evidence that may support future theoretical, empirical, and policy-oriented inquiry. Following sections are Literature Review (1), Methodology and Data (2), Results and Discussion (3) and Concluding paragraphs.

2 LITERATURE REVIEW

Cyber risk in financial institutions has become an increasingly prominent topic due to the sector's rapid digitalization and heightened exposure to interconnected technological infrastructures. As financial entities adopt cloud services, open banking, and advanced analytics, their risk surface expands accordingly, intensifying operational, reputational, and systemic vulnerabilities (Brando et al., 2022; Woods & Böhme, 2021). Research consistently shows that inadequate cybersecurity investment amplifies the likelihood and consequences of cyber incidents, resulting in financial losses and broader societal harm (Rashid et al., 2021). Despite this, the literature remains fragmented, reflecting contributions from information systems, economics, regulation, and organizational studies.

Cybersecurity in financial institutions involves safeguarding critical data, ensuring transactional integrity, and maintaining business continuity amid increasingly sophisticated cyber threats. These range from malware and phishing to advanced persistent threats, each capable of disrupting essential financial operations. Regulatory perspectives highlight the shift toward risk-based approaches, emphasizing resilience, operational continuity, and sector-wide coordination (Crisanto et al., 2023). The COVID-

19 pandemic further accelerated digital adoption while exposing the limitations of perimeter-based security models and reinforcing the shift toward zero-trust and resilience-oriented frameworks (Ahmad et al., 2021). The financial implications extend well beyond technology, affecting institutional reputation, market value, and long-term sustainability.

A growing stream of research has examined the financial sector's systemic exposure to cyber risk. Empirical analyses demonstrate how major incidents, such as the SWIFT Bangladesh Bank breach, generate cascading effects across financial networks. Studies also highlight the need for more robust causal models capable of capturing underlying determinants such as institutional maturity and threat exposure. However, evidence linking specific cybersecurity measures to measurable financial or operational outcomes remains limited, revealing a persistent empirical gap. Emerging technological infrastructures (particularly those associated with Industry 4.0, 5.0 and AI) add additional layers of complexity, as open architectures expand vulnerabilities across interconnected systems.

Cybersecurity spending represents a significant portion of IT budgets in financial institutions, yet its effectiveness is subject to debate. While large investments indicate growing awareness of cyber threats, studies show that higher spending does not always correlate with reduced incident frequency, partly due to reverse causality and confounding effects (Woods & Böhme, 2021). Cost structures encompass both direct expenditures and indirect consequences including reputational damage and regulatory penalties. Despite the importance of economic evaluation, cost–benefit analyses remain underdeveloped. Recent approaches such as return on security investment (ROSI) and cyber insurance pricing aim to address this gap, while analyses of capital versus operational expenditures suggest that accounting valuations often overestimate the true economic value of cybersecurity investments.

Governance frameworks are increasingly recognized as essential components of effective cybersecurity management. Research emphasizes board-level accountability, third-party risk oversight, staff training, and institutional culture as foundational elements of cyber resilience. Nonetheless, existing reference models often lack operational specificity, underscoring the need for clearer procedural guidance. Regulatory frameworks such as PCI-DSS and the Bank Secrecy Act define baseline requirements for data protection and incident reporting, while international bodies (i.e. BIS, IMF, and

OECD) stress information sharing and capacity building to mitigate systemic risk. Recent global assessments, such as those conducted by the WEF and ITU, highlight cybersecurity as a top-tier global risk and point to rising ransomware, supply-chain disruptions, and infrastructure attacks.

At the legislative level, measures such as the GDPR, ENISA guidelines, and the EU's NIS 2 Directive have increased compliance obligations, introduced standardized breach reporting, and expanded oversight mechanisms. Nevertheless, cross-jurisdictional divergences persist, particularly regarding technical implementation and reporting practices. Scholarly work indicates that much policy-oriented literature still prioritizes descriptive guidance over evaluative assessment, leaving significant room for empirical research on regulatory effectiveness. Additionally, studies examining cyber disclosures reveal how investors respond to transparency and tone, linking cybersecurity to broader corporate governance dynamics.

3 METHODOLOGY & DATA

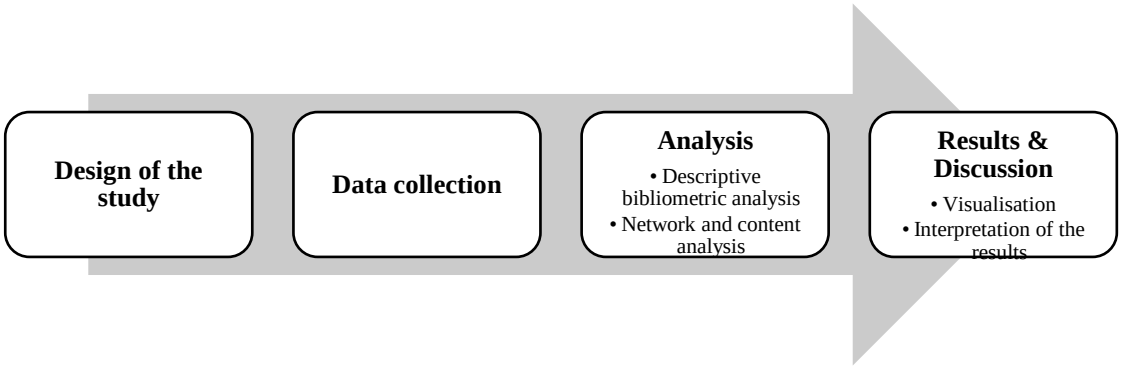
Cyber risk has emerged as a critical challenge for financial institutions as their reliance on digital infrastructures deepens. Banks, insurers, and other financial entities face a widening spectrum of threats (data breaches, ransomware attacks, disruptions of core financial infrastructure, etc.), each carrying operational, reputational, and potentially systemic consequences. Although academic and policy discussions on cybersecurity in finance have expanded considerably, the evolution, structure, and dominant themes of this research landscape remain insufficiently understood. To address this gap, this study employs a bibliometric and text mining approach to analyse how cybersecurity scholarship in the financial sector has developed over time. The analysis is guided by two research questions: (1) What are the overall trends in academic interest in cyber risk in financial institutions, and how do countries, journals, and authors contribute to this field? (2) What are the most influential concepts and theoretical frameworks in cybersecurity research on financial institutions, and how have they evolved?

The dataset was compiled from the Web of Science and imported into RStudio for processing. After conversion into the required analytical format, descriptive analyses were conducted to map annual publication trends, leading scholars and journals, institutional productivity, and citation patterns. Thematic structures were examined using

keyword co-occurrence networks to identify conceptual clusters. Co-citation and bibliographic coupling techniques were then applied to uncover relationships among publications. Finally, trend analysis traced the evolution of keywords and thematic trajectories across the study period. This methodological strategy provides a systematic overview of the intellectual and thematic development of cybersecurity research in the financial sector, by combining bibliometric mapping with text mining. It allows for an integrated assessment of how the field has matured, where conceptual boundaries have shifted, and which research directions have gained prominence.

Figure 1

Methodology design



Source: prepared by the authors

The dataset for this study was obtained exclusively from the Web of Science (WoS), selected for its broad and rigorous coverage of high-quality, peer-reviewed publications. The search spanned the period from January 1, 2000, to June 16, 2025, and was restricted to journal articles, conference proceedings, reviews, and book chapters. To maintain analytical consistency, only English-language documents were included. Bibliometric processing and scientific mapping were carried out using the bibliometrix package in R, which provides advanced tools for analysing and visualizing bibliographic data (Aria & Cuccurullo, 2017). The search strategy relied on two sets of keywords—one focused on cybersecurity and the other on the financial sector—to ensure comprehensive retrieval of relevant publications (Table 1).

Table 1

Descriptive analysis

Search timeframe	2000 – June 2025
Document types	Journal articles, conference proceedings, reviews, book chapters
Language	English
Fields	Title, Abstract, Keywords, Authors, Source, References
Thematic Area	**Sample Keywords**
Cybersecurity	"cybersecurity", "cyber security", "cyber-security" OR "cyber risk", "cyber attack", "cyber-attack", "cyber threat", "cyber harm", "information security", "data breach", "IT security", "cyber resilience", "digital security"
Financial sector	"bank*", "financial institution*", "financial sector", "insurance compan*", "commercial bank*", "central bank*", "fintech", "financial service*", "banking vulnerability"

Source: prepared by the authors

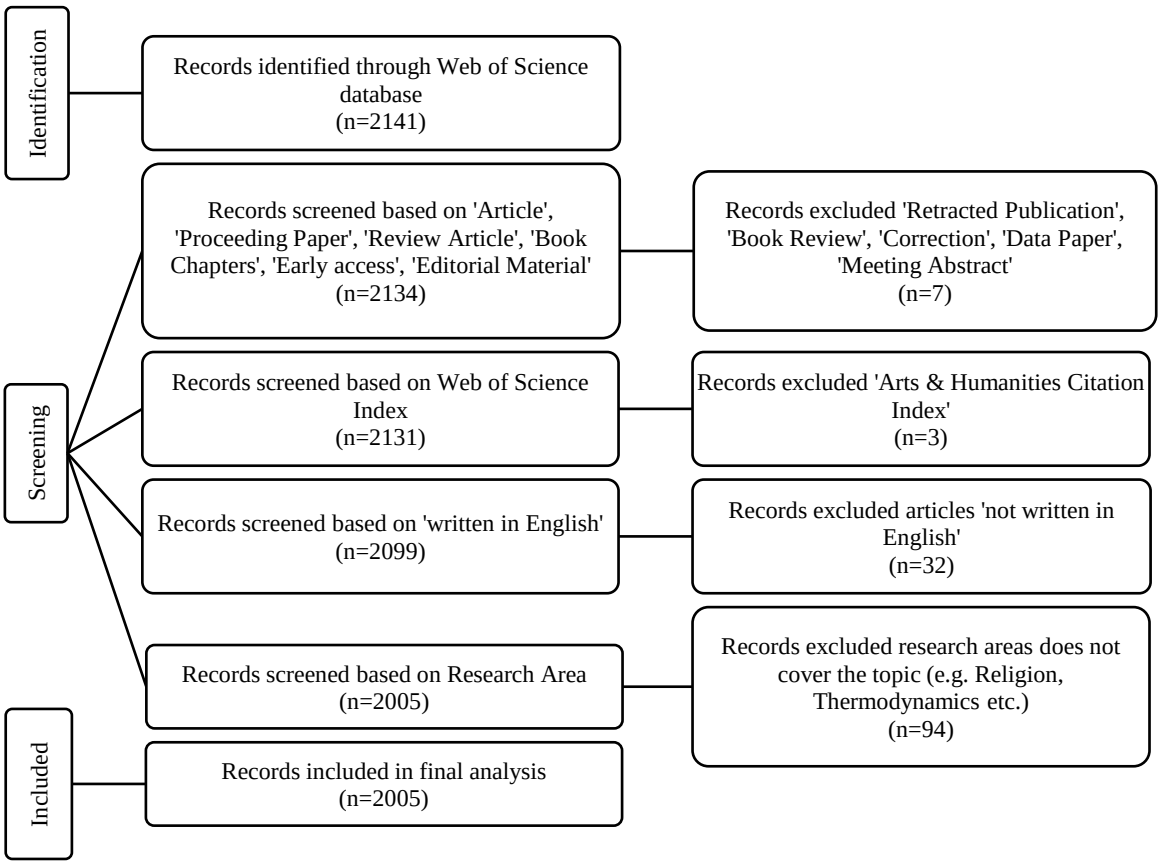
The cybersecurity-related terms alone yielded 86,936 records, whereas the financial-sector terms returned 587,860 records. When these two thematic dimensions were combined via Boolean logic, the search resulted in a total of 2,141 documents, which formed the initial dataset for further screening and analysis. To ensure a transparent and replicable data screening process, we adhered to the PRISMA 2020 guidelines (Preferred Reporting Items for Systematic reviews and Meta-Analyses) (Page et al., 2021). The multi-step filtering procedure, illustrated in Figure 2, outlines the inclusion and exclusion criteria used to refine the dataset:

- Only specific document types were included: 'Article', 'Proceedings Paper', 'Review Article', 'Book Chapters', 'Early Access', and 'Editorial Material'. Nonresearch-oriented entries such as 'Retracted Publications', 'Book Reviews', and 'Data Papers' were excluded (n=7).
- Records not indexed in the core Web of Science indices, particularly those from the 'Arts & Humanities Citation Index', were removed (n=3).
- Only publications written in English were retained, and 32 non-English entries were excluded.
- Finally, documents not aligned with the relevant research areas—such as those covering unrelated topics such as religion or thermodynamics—were excluded (n=94).

After this multistep screening, the final dataset consisted of 2,005 documents suitable for bibliometric and content analysis.

Figure 2

PRISMA flowchart



Source: prepared by the authors based on Page et al. (2021)

The final corpus included 2,005 publications spanning the period from 2000 to 2025, derived from 1,219 distinct sources (journals, books, etc.). The structure of the dataset is summarized in Table 2.

Table 2

Structure of the final dataset

Description	Results
Documents	2005
Period	2000-2025
Sources (Journals, Books, etc.)	1219
Keywords Plus (ID)	1308
Author's Keywords (DE)	5845
Average citations per doc	11.94
Authors	5964

Article	953
Article; Book Chapter	50
Article; Early access	26
Article; Proceedings Paper	22
Editorial Material	11
Proceedings Paper	895
Review	46
Review; Early Access	2

Source: prepared by the authors

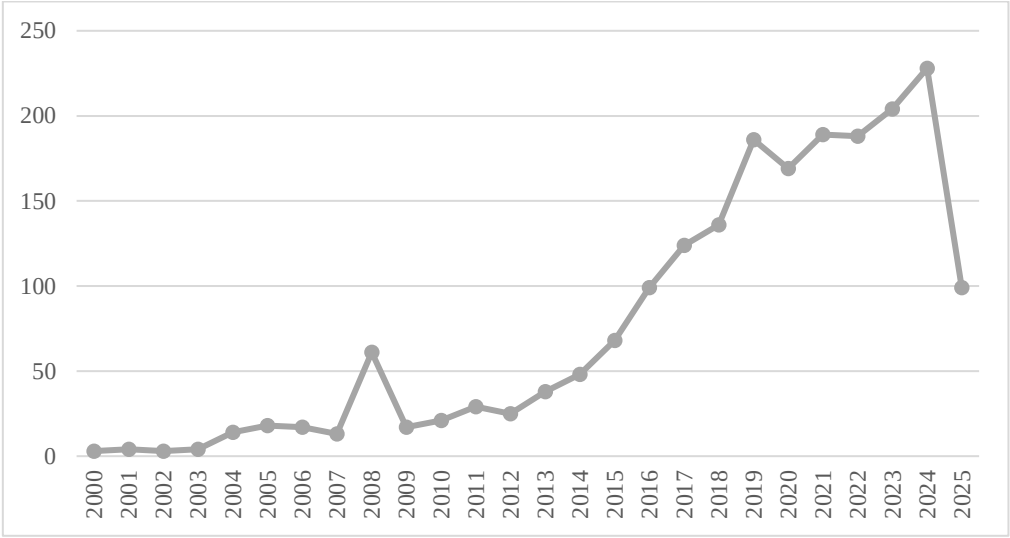
The analysis consisted of descriptive bibliometric assessment alongside network and content analysis (Figure 2). Bibliometric indicators were employed to map publication trends, citation patterns, and authorship structures. Network analysis was then used to identify co-authorship relations, co-citation networks, and thematic clusters. Complementing this, content analysis—supported by text mining—served to extract dominant themes and trace shifts in research focus over time. The resulting outputs were visualized and interpreted to provide an integrated understanding of how scholarship on cybersecurity in the financial sector has evolved.

4 RESULTS & DISCUSSION

Figure 3 illustrates the steady increase in studies addressing cybersecurity in the financial sector between 2000 and 2025. This consistent upward trajectory reflects the expanding academic interest driven by the digitalization of financial services, the rise of fintech, and the implementation of more stringent regulatory frameworks, all of which have positioned cybersecurity as a central concern for both researchers and practitioners. Although publication volume provides an initial indication of the field's development, it offers limited insight into the substantive themes and intellectual structures shaping the literature. To capture these deeper dynamics, this study applies a comprehensive bibliometric and content analysis to explore the geographical distribution of research output, leading journals and publication networks, patterns of authorship and collaboration, citation structures, influential works, and keyword co-occurrence trends.

Figure 3

The number of studies published from 2000 to 2025



Source: prepared by the authors

4.1 Distribution of publications related to cybersecurity in the financial sector across various source types

Table 3 summarizes the most productive publication venues with at least eleven articles between 2000 and 2025. Although the dataset contains 1,219 unique sources, bibliometric indicators (such as the h-index) can be calculated for only 718, underscoring limited citation activity for many outlets. Notably, 931 sources published a single article, and 162 published exactly two. This pattern indicates high dispersion of research across a broad range of journals, reflecting the interdisciplinary nature of cybersecurity scholarship in financial contexts.

Table 3

Distribution of publications across various sources (2000-2025); sources with eleven or more publications

Sources	No. of articles	Total citations	h_index	g_index	m_index	Publication year start
Computers & Security	45	1663	21	40	0.84	2001
IEEE Access	44	1308	15	36	1.67	2017
Information and Computer Security	21	365	10	19	0.91	2015
Journal of Information Security and Applications	19	736	10	19	1.11	2017
Information Security Journal	18	73	6	7	0.35	2009
International Journal of Information Security and Privacy	16	84	4	9	0.21	2007
International Journal of Information Security	15	110	7	10	0.41	2009
Sensors	14	168	9	12	0.53	2009

Scientific Reports	13	183	5	13	0.56	2017
Applied Sciences - Basel	11	104	5	10	0.63	2018

Source: prepared by the authors

Citation-based indicators offer deeper insight into journal influence. The h-index captures how many articles have received at least the same number of citations. The g-index places more emphasis on highly cited papers, while the m-index normalizes the h-index by years of publication activity. Together, these metrics highlight structural differences between long-standing and newer journals in the domain.

4.2 The most productive countries

The corresponding authors come from 111 countries. Of these, 21 are represented by a single publication, and 25 contributed five or fewer, indicating globally dispersed but often limited engagement with the topic. Table 4 lists the five most productive countries based on corresponding-author affiliation, showing total publications, their frequency, and the balance between single-country publications (SCP) and internationally co-authored papers (MCP). The MCP ratio reflects each country's level of international collaboration.

Table 4.

The most productive countries on the basis of the corresponding author affiliation

Country	Articles	Freq	Single country publication	Multiple country publication	MCP_Ratio
USA	288	0.146	217	71	0.25
INDIA	219	0.111	203	16	0.07
CHINA	188	0.095	137	51	0.27
UNITED KINGDOM	117	0.059	81	36	0.31
RUSSIA	60	0.030	55	5	0.08

Source: prepared by the authors

The United States leads the dataset with 288 publications (14.6%), along with substantial international collaboration reflected in its MCP ratio of 0.25. India follows with 219 publications (11.1%) but exhibits a markedly low MCP ratio (0.07), indicating predominantly domestic research activity. China contributes 188 publications (9.5%) and demonstrates balanced engagement across domestic and international collaborations. The United Kingdom shows strong collaborative orientation with an MCP ratio of 0.31. Saudi

Arabia displays the highest collaboration intensity among the top contributors, with half of its publications co-authored internationally. Countries such as South Africa, Australia, and Ukraine exhibit moderate integration into global research networks, with MCP ratios between 0.13 and 0.33.

4.3 Top contributing authors

Table 5 presents leading authors by total publication output and by fractionalized authorship, which adjusts contributions based on the number of co-authors. The first column lists authors with more than seven publications. The second offers a more equitable perspective on individual contributions. For instance, Von Solms B. has the highest fractional score (3.67), indicating a strong individual research footprint, while Liu Y. ranks highly in both raw and fractional counts.

Table 5

The most productive authors

Authors	Articles	Total citations	Authors	Articles Fractionalized
LIU Y	12	225	VON SOLMS B	3.67
GUPTA S	8	123	LIU Y	3.44
CHEN H	8	109	BATAEV AV	3
LIU X	8	38	IFINEDO P	3
ALJAMEEL SS	7	44	OZILI PK	3
CREESE S	7	61	GUPTA S	2.83
GRIMA S	7	3	JANSEN J	2.7
GUPTA M	7	175	GORIAN E	2.5
LI Y	7	186	WAWRZYNIAK D	2.5
WANG J	7	190	GUPTA BB	2.42

Source: prepared by the authors

The contrast between total and fractionalized authorship highlights different forms of scholarly impact. Some authors combine high productivity with strong individual contributions, while others appear primarily in highly collaborative networks. To further assess productivity patterns, Lotka's Law was applied. The estimated beta coefficient of 3.45 indicates a steeper decline in author productivity than the theoretical baseline of 2, suggesting that only a small group repeatedly contributes to this field. Despite this deviation, the model shows strong empirical fit ($R^2 = 0.992$), and the Kolmogorov–Smirnov test ($p = 0.124$) confirms that the observed distribution is not significantly different from Lotka's theoretical formulation.

4.4 Co-citation network

Table 6 identifies the most influential references within the dataset based on local citation counts. These works have been cited most frequently by other publications within this corpus and therefore represent the core intellectual foundations of cybersecurity research in financial institutions.

Table 6

The most locally cited authors

Authors & Year	Topic	Citations
Biener, C., Eling, M., & Wirfs, J. H. (2015)	Insurability of cyber risk: An empirical analysis.	29
Davis, F. D. (1989)	Perceived usefulness, perceived ease of use, and user acceptance of information technology	29
Gordon, L. A., & Loeb, M. P. (2002)	The economics of information security investment	23
Herath, T., & Rao, H. R. (2009)	Protection motivation and deterrence: a framework for security policy compliance in organisations	22
Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004)	The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers	19

Source: prepared by the authors

The prominence of these foundational contributions reflects the central theoretical and empirical models shaping contemporary scholarship, including economics of information security, cyber risk insurability, user compliance, and the market effects of breach disclosures.

4.5 Co-occurrence analysis

Table 7 displays the most frequent terms drawn from Author's Keywords and Keywords-Plus, after harmonizing synonym variants through the bibliographic synonym list. This ensures consistency by merging equivalent terms such as cybersecurity and cyber security. Author's Keywords represent explicit topical focus, while Keywords-Plus derive from the cited references and thus capture the conceptual background of the field. Cyber security appears most frequently among Author's Keywords (550 occurrences), followed by information security (202). The Keywords-Plus dataset reinforces the same

conceptual core, indicating alignment between authors' thematic intentions and the broader intellectual context of their work.

Table 7

Keyword occurrence analysis

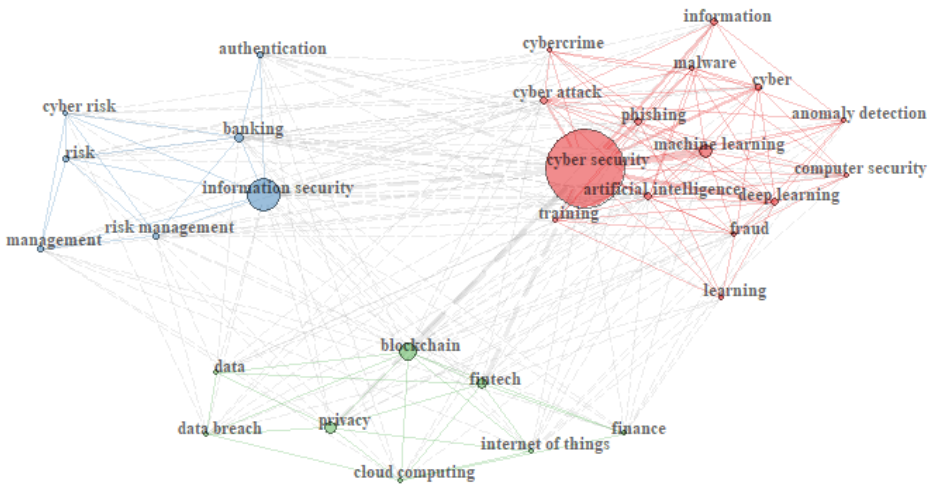
Author's Keywords	Occurrences	Keywords-Plus	Occurrences
CYBER SECURITY	550	SECURITY	86
INFORMATION SECURITY	202	MODEL	83
BLOCKCHAIN	97	MANAGEMENT	56
MACHINE LEARNING	93	IMPACT	49
FINTECH	59	INTERNET	46
PRIVACY	59	RISK	40
DEEP LEARNING	49	PRIVACY	38
CYBER ATTACK	48	SYSTEMS	38
PHISHING	46	FRAMEWORK	36
ARTIFICIAL INTELLIGENCE	44	INFORMATION	35

Source: prepared by the authors

Figure 4 presents the keyword co-occurrence network based on Author's Keywords. Node size corresponds to frequency, and edge thickness reflects co-occurrence strength.

Figure 4

Keyword Co-occurrence network



Source: prepared by the authors

Clusters were identified via the Louvain community detection algorithm and color-coded accordingly:

- The red cluster captures cybersecurity and artificial intelligence, including themes such as machine learning, cyber attacks, phishing, and malware.
- • The blue cluster centers on information security and risk management, covering institutional security practices and authentication.
- • The green cluster reflects emerging technologies such as blockchain, fintech, and cloud computing, indicating growing interest in digital financial infrastructures.

The interconnectedness between clusters demonstrates the interdisciplinary nature of cybersecurity research, particularly the link between technical threats (e.g., phishing, malware), systemic risk, and the adoption of emerging technologies.

5 CONCLUSION

This study offers a systematic bibliometric and content-based assessment of cybersecurity research in the financial sector, particularly within banking and insurance. By combining mapping techniques with thematic analysis, it traces the evolution of scholarly interest, identifies key intellectual clusters, and highlights areas that require deeper investigation. The findings reaffirm that cybersecurity has become a central strategic priority with regulatory, economic, and societal relevance. The results illustrate a broad recognition of the systemic nature of cyber risks, which increasingly transcend national boundaries and rely on sophisticated technological vectors. Yet empirical evidence on the effectiveness of cybersecurity investments remains scarce, and the absence of established models for evaluating financial returns on security spending limits the field's capacity to guide policy. Governance practices, including institutional oversight and organizational readiness, appear crucial for enhancing resilience, while regulatory heterogeneity across jurisdictions reflects the ongoing challenge of harmonizing cybersecurity standards despite initiatives such as the GDPR, ENISA guidelines, and the NIS 2 Directive.

Patterns of country productivity reveal both concentration and fragmentation. A small group of nations dominates output, but levels of international collaboration differ substantially. High collaboration ratios in countries with modest publication volumes indicate the importance of global networks, whereas low ratios in major contributors point to untapped opportunities for cross-border cooperation. Publication dispersion across a

wide range of journals further demonstrates the interdisciplinary reach of the field and the need for researchers to engage with diverse outlets.

The study is limited by its reliance on the Web of Science and English-language publications, which may exclude relevant scholarship. The exclusive use of bibliometric and text mining techniques also restricts the exploration of theoretical and causal dimensions. Future research should prioritize interdisciplinary frameworks that integrate technical, economic, and regulatory perspectives, as well as empirical evaluations of cybersecurity effectiveness, cost structures, and institutional responses to cyber policy.

FUNDING

This paper is the output of a research project supported by the the Slovak Research and Development Agency under Contract no. VV-MVP-24-0272.

DECLARATION OF COMPETING INTEREST

The authors hereby declare no conflicts of interest.

CONSENT FOR PUBLICATION

The authors are willing for publication of this manuscript.

DATA AVAILABILITY

The data that support the findings of this study are available from the authors upon reasonable request.

AUTHORS CONTRIBUTIONS

CRediT: **Marek Pekarčík**: Conceptualization, Methodology, Software, Writing – original draft. **Jakub Sopko**: Conceptualization, Software, Writing – original draft. **Leoš Šafár**: Conceptualization, Formal analysis, Writing – review & editing.

GENERATIVE AI STATEMENT

During the preparation of this work the authors used Rubriq (former CURIE) in order to improve the quality of the writing and corrections. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article.

REFERENCES

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536. https://doi.org/10.37896/jxu14.7/174

Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022, May). Cyber security threats on digital banking. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICAIC53980.2022.9896966

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of informetrics*, *11*(4), 959-975. https://doi.org/10.1016/j.joi.2017.08.007

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, *78*, 102670. https://doi.org/10.1016/j.techsoc.2024.102670

Barcellos-Paula, L., Gil-Lafuente, A. M., & Merigó, J. M. (2025). Research on cybersecurity and business: A bibliometric review (2004-2023). *Cuadernos de Gestión*, *25*(1), 19-36. https://doi.org/10.5295/cdg.242288lb

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), 131-158. https://doi.org/10.1057/gpp.2014.19

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund. https://doi.org/10.5089/9781484360750.001

Brando, Danny and Kotidis, Antonis and Kovner, Anna and Lee, Michael and Schreft, Stacey L., Implications of Cyber Risk for Financial Stability (May 1, 2022). *FEDS Notes* No. 2022-05-12. https://doi.org/10.17016/2380-7172.3077

Brho, M., Jazairy, A., & Glassburner, A. V. (2025). The finance of cybersecurity: Quantitative modeling of investment decisions and net present value. *International Journal of Production Economics*, *279*, 109448. https://doi.org/10.1016/j.ijpe.2024.109448

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70-104. https://doi.org/10.1080/10864415.2004.11044320

Crisanto, J., Umebara, P., & Prenio, A. (2023). Banks' cyber security–a second generation of regulatory approaches. *Financial Stability Institute FSI Insights on Policy Implementation*, (50). https://www.bis.org/fsi/publ/insights50.pdf

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEe Access*, *11*, 125138-125158. https://doi.org/10.1109/ACCESS.2023.3327016

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340. https://doi.org/10.2307/249008

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438-457. https://doi.org/10.1145/581271.581274

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, *18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Kaffenberger, L., & Kopp, E. (2019). *Cyber risk scenarios, the financial system, and systemic risk assessment*. Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Kaffenberger_Cyber_Risk_Scenarios_final1.pdf

Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

Matejka, V., Soto, J., & Franco, M. (2021). A framework for the definition and analysis of cyber insurance requirements. *Master Project, University of Zurich, Communication Systems Group, Department of Informatics, Zurich, Switzerland*. https://files.ifi.uzh.ch/CSG/staff/franco/extern/theses/MAP-VM-JAHS.pdf

Pacelli, V. (2025). *Systemic Risk and Complex Networks in Modern Financial Systems* (p. 412). Springer Nature. https://doi.org/10.1007/978-3-031-64916-5

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, *372*.

Rashid, Z., Noor, U., & Altmann, J. (2021). Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. *Future Generation Computer Systems*, *124*, 436-466. https://doi.org/10.1016/j.future.2021.05.033

Sheehan, B., Murphy, F., Kia, A. N., & Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*, *24*(12), 1619-1638. https://doi.org/10.1080/13669877.2021.1900337

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, 22(4), 239-309. https://doi.org/10.1057/s41283-020-00063-2

Woods, D. W., & Böhme, R. (2021). SoK: Quantifying cyber risk. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 211-228). IEEE. https://doi.org/10.1109/SP40001.2021.00053

World Economic Forum. 2025. The Global Risks Report 2025 – 20th Edition. Available at: <https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf>

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Pekarčík, M., Sopko, J., & Šafár, L. (2025). CYBERSECURITY IN FINANCIAL INSTITUTIONS: A BIBLIOMETRIC AND THEMATIC ANALYSIS OF GLOBAL RESEARCH (2000–2025). *Veredas Do Direito*, 22(7), e223815. https://doi.org/10.18623/rvd.v22.n7.3815