Balkans JETSS (2025) 2: 90-102
DOI: https://doi.org/10.31410/Balkans.JETSS.2025.8.2.90-102

Review Article

Unpacking Cybersecurity in Financial Research: A Systematic Mapping Approach

Leoš Šafár[1]
Michal Mešťan[2]
Jakub Sopko[3]

Received: October 10, 2025 / Revised: December 29, 2025 /
Accepted: December 30, 2025 / Published: December 30, 2025

Abstract: *This study presents a comprehensive bibliometric and content analysis of cybersecurity research in financial institutions covering the period from 2000 to 2025. By applying the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology, we systematically identified and screened 2,005 peer-reviewed articles indexed in the Web of Science Core Collection. The review focuses on cybersecurity within the financial system, particularly in the banking and insurance sectors, and maps research trends, innovation gaps, and thematic evolutions in this domain. Thematic analysis on the basis of keyword co-occurrence identified three distinct clusters. The first cluster focuses on cybersecurity and artificial intelligence, including keywords such as cyber security, phishing, malware, and machine learning, highlighting AI-driven threat detection and digital defense mechanisms. The second cluster focuses on institutional risk management and information security, emphasizing governance, authentication, and systemic controls within financial institutions. The third cluster involves emerging digital technologies, such as blockchain, cloud computing, and FinTech, underscoring the technological innovations that shape financial services and data protection frameworks. Despite growing research output and increasing attention to cyber risk from both academic and regulatory perspectives, the field remains fragmented, with limited empirical evaluation of cybersecurity investment effectiveness. By combining PRISMA guidelines with bibliometric mapping, this study offers a structured and interdisciplinary overview of cybersecurity research in financial institutions. It highlights key research frontiers and calls for deeper empirical inquiry, particularly on systemic financial risk, cross-sector governance, and cybersecurity policy design.*

Keywords: *Cybersecurity, Financial institutions, PRISMA, Bibliometric analysis, Operational risk, Cyber resilience*

JEL Classification: G21 · M15 · O33

✉ leos.safar@tuke.sk
[1] Technical University of Košice, Faculty of Economics, Department of Banking and Investment, Němcovej 32, 040 01 Košice, Slovakia
[2] Matej Bel University in Banská Bystrica, Faculty of Economics, Department of Finance and Accounting, Tajovského 10, 975 90 Banská Bystrica, Slovakia
[3] Technical University of Košice, Faculty of Economics, Department of Banking and Investment, Němcovej 32, 040 01 Košice, Slovakia

1. INTRODUCTION

The accelerating digital transformation of financial systems has redefined how banks, insurers, and related institutions operate, interact with customers, and manage risk. Developments such as mobile banking, algorithmic trading, blockchain-based settlement, and cloud computing have increased operational efficiency and broadened access to services, yet they have also expanded the attack surface for malicious actors. The frequency, scale, and sophistication of cyber threats, including phishing, ransomware, advanced persistent threats (APTs), and large-scale data breaches that jeopardize both institutional viability and systemic stability, have increased (Kemp et al., 2021). The International Monetary Fund (IMF) estimates that severe cyber incidents could cost the global banking sector nearly 9% of its annual profits, underscoring the economic magnitude of the challenge (Bouveret, 2018). The multidimensional nature of cyber risk, which spans technical vulnerabilities, governance failures, and regulatory shortcomings, complicates mitigation efforts. Empirical evidence shows that governance structures, such as the presence of a Chief Risk Officer or dedicated IT committees, can moderate the effectiveness of cybersecurity disclosure and influence bank performance (Elsayed et al., 2024). In parallel, emerging technologies such as artificial intelligence (AI), blockchain, and FinTech applications are transforming both security capabilities and threat vectors (Brando et al., 2022; Sethi et al., 2025; Woods & Böhme, 2021). While FinTech innovations can increase efficiency and expand financial inclusion, they also introduce operational complexities and, in some contexts, short-term profitability pressures due to high implementation costs and intensified competition (Elmahdy et al., 2025; Sethi et al., 2025).

Cybersecurity threats in the banking sector have risen sharply alongside the rapid digitalization, with the IMF reporting a post-COVID-19 doubling of attacks and incidents in finance, which now comprise nearly one-fifth of all cases. Severe cyber incidents now cost up to $2.5 billion annually, with additional reputational and operational losses (International Monetary Fund, 2024). Sulong et al. (2025) analysed U.S. bank data during the period 1998-2018 and showed that heightened cybersecurity risk is positively associated with increased bank risk-taking, especially in smaller, financially vulnerable institutions and those under greater competitive pressure or facing high deposit withdrawals. Factors such as disclosure tone, IT investment intensity, and goodwill condition this relationship, underscoring the complex interplay between cyber risk exposure and strategic behavior in the banking sector.

The policy environment is also evolving. Regulatory bodies, including the Basel Committee, the IMF, and the OECD, have integrated cybersecurity into prudential frameworks, advocating risk-based oversight and systemic resilience (Aldasoro et al., 2020; OECD, 2022; Ravikumar, 2025). PRISMA-based reviews in related domains, such as sustainable finance and central bank digital currencies (CBDCs), highlight the methodological value of structured evidence synthesis in identifying thematic trends, regulatory priorities, and innovation gaps (Galletta et al., 2024; Prodan et al., 2024). The PRISMA-based and bibliometric reviews examine fintech innovation, digital finance, operational risk, or central bank digital currencies, but cybersecurity is typically treated as a supporting topic within these broader themes. In contrast, this study offers a systematic mapping focused exclusively on cybersecurity in financial institutions, with emphasis on banking.

Addressing this gap requires an integrative approach that combines bibliometric analysis with thematic synthesis to uncover research frontiers and fragmentation patterns. This study applies the PRISMA methodology to 2,005 Web of Science–indexed publications (2000–2025) to map the intellectual and conceptual landscape of cybersecurity in financial institutions, with an emphasis on banking and insurance. By identifying clusters of research activity, tracing the evolution of

themes, and pinpointing underexplored areas, we contribute a sector-specific evidence base that can inform academic inquiry, regulatory design, and institutional strategies aimed at strengthening cyber resilience.

In this study, the terms “cybersecurity” and “cyber security” are used interchangeably.

This study addresses four research questions:

- **Research Question One (RQ1):** Which journals are the most influential in the field of cybersecurity research within financial institutions?
- **Research Question Two (RQ2):** What are the major themes and topics emerging from cybersecurity research in the financial sector?
- **Research Question Three (RQ3):** Which of the most influential articles shape cybersecurity research in financial institutions?
- **Research Question Four (RQ4):** What are the future research directions for cybersecurity in the financial sector?

The remainder of this article is structured as follows. Section 2 reviews the relevant literature, positioning this study within existing research on cybersecurity in financial institutions. Section 3 outlines the design and methodological approach, including the PRISMA flowchart and bibliometric techniques employed. Section 4 presents the results of the science mapping and thematic analysis. Section 5 discusses the implications of the findings and proposes directions for future research. Section 6 concludes the paper by summarizing key contributions and highlighting policy and practice implications.

2. LITERATURE REVIEW

Research on cybersecurity in financial institutions has broadened from technical safeguards toward governance, disclosure, and systemic-risk perspectives as digitalization has accelerated. Foundational texts document rising costs and the need for coherent frameworks, whereas policy reports emphasize resilience and coordinated oversight across the sector. These strands frame three concise themes our mapping will interrogate (Bouyon & Krause, 2018; Daimi & Peoples, 2021).

2.1. Cybersecurity Threat Landscape in Finance

Recent reports underscore that cyber incidents can jeopardize financial stability, not merely firm-level operations. The Bangladesh Bank/SWIFT case is widely cited as a systemic wake-up call, and international bodies have since warned that a major cyberattack could precipitate a financial crisis (Maurer & Nelson, 2021). Foundational overviews also stress that, despite proliferating standards and spending, the cost of attacks continues to rise, requiring continual adaptation of defenses (Daimi & Peoples, 2021). At the macro level, the IMF’s Global Financial Stability Report (International Monetary Fund, 2024) treats cyber risk as an emerging concern for macrofinancial stability, placing it firmly on the financial stability agenda.

2.2. Governance, Regulation, and Risk Management

Policy analysis recommends shifting emphasis from ad hoc protection to resilience and clarifies three pillars - governance, risk management, and capability, alongside concrete needs such as convergent incident-reporting taxonomies and better statistics (Bouyon & Krause, 2018). Sectoral overviews highlight that threats and under-reporting expanded markedly in financial services,

motivating organization-wide risk management rather than purely technical fixes (Taplin, 2016). At the firm level, empirical evidence links cybersecurity disclosure to real economic relationships with major customers, indicating that external stakeholders value a stronger cybersecurity posture (Nelson & Wang, 2024). Complementary practice guidance urges finance and accounting professionals to move beyond passive awareness toward structured, risk-based programs aligned with the NIST Cybersecurity Framework (Pendley, 2018).

2.3. Thematic Trends and Research Gaps

Across the literature, three themes recur: (i) evolving attacks surface with digital transformation; (ii) enterprise risk management and disclosure; and (iii) policy and supervisory architectures for resilience. Daimi and Peoples (2021) map enterprise risk frameworks and identity/operations management as organizing concepts for research and practice. The broader AI-driven digital economy heightens exposure and calls for adaptation, reinforcing the need to connect technology, governance, and policy in financial-sector settings (Makarenko et al., 2023; Pacelli, 2025). Moreover, policy analysts describe persistent fragmentation and coordination gaps, and our science-mapping approach is designed to surface and structure these gaps (Maurer & Nelson, 2021).

3. DESIGN AND METHOD

This study employs the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology to ensure a transparent, rigorous, and replicable review process. Although PRISMA originated in health sciences (Liberati et al., 2009; Moher et al., 2009), it has been widely adopted in management, finance, and information systems research for structuring systematic reviews (Cooper et al., 2018; Tranfield et al., 2003). The method is particularly suited to synthesizing and mapping large bodies of academic literature, enabling the identification of thematic trends, intellectual structures, and research gaps. We use updated PRISMA guidelines (Page et al., 2021) and combine them with science mapping techniques implemented in the bibliometrix package for R (Aria & Cuccurullo, 2017). This integration allows for both qualitative synthesis and quantitative bibliometric analysis, providing a comprehensive view of how cybersecurity research in financial institutions has evolved over time. Following the structured approach of PRISMA, our review proceeded through four sequential phases (more detailed in Figure 2).

1. *Identification:* The initial search was conducted in the Web of Science Core Collection database, which was selected for its comprehensive indexing of peer-reviewed literature and compatibility with bibliometric tools. Search terms were developed to capture a broad scope of studies related to cybersecurity in financial institutions, including combinations of "cybersecurity" OR "information security" OR "cyber risk" AND "bank*" OR "insurance" OR "financial institution*". The search was limited to journal articles, conference papers, and review papers published in English between January 2000 and June 2025 (see more details in Table 1).
2. *Screening:* All records were reviewed by title, abstract, and keywords to assess relevance. Studies unrelated to cybersecurity in financial contexts, such as those focusing on non-financial industries or general IT security without sectoral application, were removed. Duplicate entries were also excluded during this stage.
3. *Eligibility:* The remaining records were examined to confirm compliance with the inclusion criteria: (i) direct focus on cybersecurity, information security, or cyber risk; (ii) explicit relevance to financial institutions (banking, insurance, or related financial services); and (iii) publication in peer-reviewed outlets. Non-English records, incomplete studies, or those lacking methodological transparency were excluded.

4. *Inclusion:* After applying the eligibility criteria, the final dataset comprised 2,005 publications. Bibliographic data were exported from Web of Science (WoS) in plain text format and processed with the bibliometrix package. The analyses included performance metrics, co-authorship networks, co-occurrence mapping of author keywords, and thematic evolution analysis. These techniques facilitated the identification of influential authors, journals, articles, and research clusters, directly addressing the study's research questions.

By combining the structured PRISMA protocol with bibliometric science mapping, this study ensures methodological transparency, replicability, and analytical depth, offering a robust synthesis of two and a half decades of cybersecurity research in financial institutions.

4. RESULTS

Figure 1 shows the annual distribution of publications on cybersecurity in financial institutions from 2000 to June 2025. Research output was minimal in the early 2000s, with a noticeable spike in 2008, followed by a decline and gradual growth until 2013. A sustained upward trend began in 2014, accelerating sharply between 2016 and 2019 and reaching its peak in 2024, with over 220 publications. The lower count in 2025 reflects mid-year data collection rather than an actual drop in research activity.

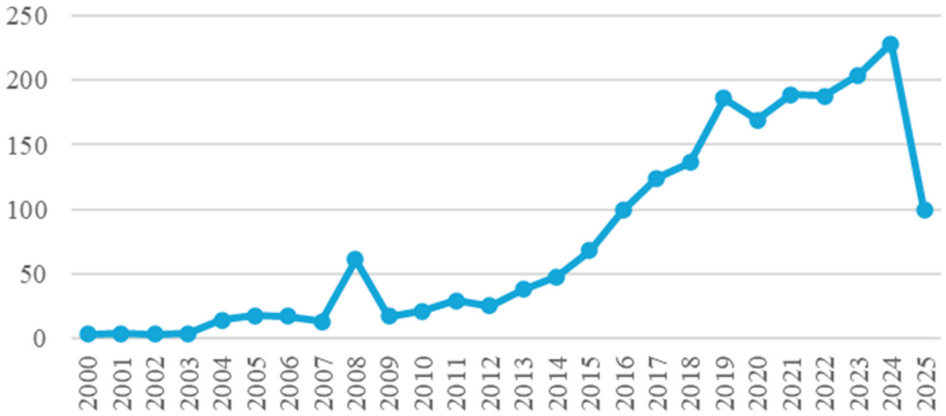

Figure 1. Total number of publications between 2000 and June 2025
Source: Own processing

Table 1 summarizes the PRISMA model applied in this study, outlining the review design, protocol, eligibility criteria, and search strategy. We combined two thematic dimensions, cybersecurity and the financial sector (Uddin et al., 2020), using predefined Boolean codes in the Web of Science Core Collection to ensure comprehensive and replicable coverage of relevant literature.

Figure 2 presents the PRISMA flow diagram summarizing the selection process for the systematic review. The initial keyword search in the Web of Science Core Collection returned 86,936 records for cybersecurity-related terms and 587,860 for financial-sector terms. When these two thematic dimensions were combined via Boolean logic, the search yielded 2,141 documents, which formed the initial dataset for screening and analysis. Following the PRISMA 2020 guidelines (Page et al., 2021) to ensure transparency and replicability, seven items, such as retracted publications, book reviews, and meeting abstracts, were removed, leaving 2,134 records. Further screening excluded three items indexed only in the Arts & Humanities Citation Index and 32 articles not

written in English, resulting in 2,099 records. The research area filter removes 94 unrelated items (e.g., works in religion or thermodynamics), producing the final dataset of 2,005 publications used for bibliometric and thematic analyses.

Table 1. PRISMA model for systematic literature review

Study design	The study conducts a literature review that synthesizes existing research through a rigorous, clearly defined, and transparent step-by-step process.
Review protocol	To reduce the risk of "biased post hoc decisions in review methods" (Liberati et al., 2009), the search criteria and corresponding keywords were defined in advance.
Eligibility criteria	The review included only articles published in peer-reviewed journals, conference proceedings, reviews, and book chapters. Studies were retrieved from the Web of Science electronic database using search codes established by the authors, and the resulting bibliometric data were subsequently mapped and clustered.
Publication type included	Peer-reviewed journals, conference proceedings, reviews, and book chapters from the Web of Science database
Publication timeframe	2000 – June 2025
Language	English
Search strategy	We have used two thematic areas: cybersecurity and financial sector. We selected the following codes to search in the WoS database: ALL= "cybersecurity" OR "cyber security" OR "cyber-security" OR "cyber risk" OR"cyber attack", "cyber-attack" OR "cyber threat" OR "cyber harm", "information security" OR "data breach" OR "IT security" OR "cyber resilience" OR "digital security" AND "bank*" OR "financial institution*" OR "financial sector" OR "insurance compan*" OR "commercial bank*" OR "central bank*" OR "fintech" OR "financial service*" OR "banking vulnerability"

Source: Own processing

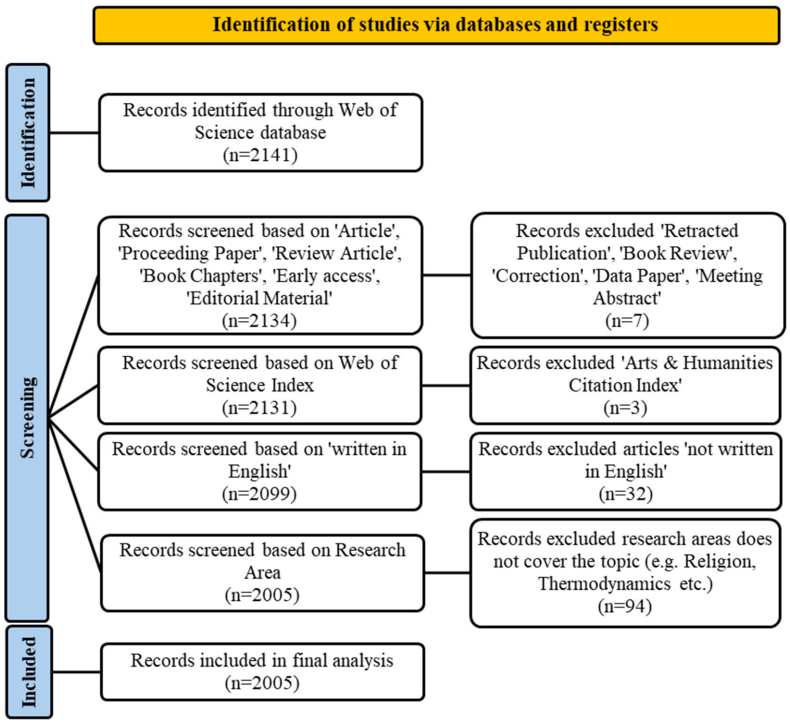

Figure 2. PRISMA flowchart for the systematic literature review

Source: Own processing

Table 2 lists the most productive and influential journals publishing on cybersecurity in financial institutions (RQ1). Computers & Security leads in output with 45 publications and an h-index of 21, followed by IEEE Access (44 publications; h-index 15) and Information and Computer Security (21 publications; h-index 10). Citation metrics such as the g-index and m-index confirm the consistent impact of these outlets over time, positioning them as core publication venues for the field. The *h*-index measures a journal's impact by counting how many articles, *h*, have at least *h* citations. The *g*-index is a similar metric that gives more weight to highly cited papers. It identifies the top *g* articles that have received a total of at least g^2 citations. To compare journals of different ages, the *m*-index is a useful adjustment. It divides the *h*-index by the number of years the journal has been published.

Table 2. Distribution of publications across influential journals

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
Financial and Credit Activity - Problems of Theory and Practice	11	16	2	2	0.33	2020

Source: Own processing

The author-keyword co-occurrence analysis (Figure 3) reveals three distinct thematic clusters shaping the field (RQ2):

1. Technological Threat Detection and AI Integration (Red cluster)
    a. This includes "cybersecurity," "artificial intelligence," "machine learning," "phishing," "fraud," and "malware," indicating strong research activity on AI-driven threat identification, anomaly detection, and predictive modeling. The high density of links in this cluster demonstrates tight conceptual integration, reflecting the sector's increasing reliance on data-driven security tools. From a policy perspective, the prominence of this cluster emphasizes the importance of regulatory frameworks that address algorithmic risk alongside operational resilience.
2. Governance, Risk Management, and Institutional Controls (Blue cluster)
    a. Centered on "information security," "risk management," and "authentication," this cluster reflects research that integrates cybersecurity with enterprise risk frameworks, authentication protocols, and systemic governance measures within financial institutions. Its centrality also underscores that cybersecurity is no longer considered as an IT function but rather one of the main pillars of financial stability and regulatory compliance, which are reinforced by regulatory initiatives that embed cybersecurity risk into capital adequacy, governance standards, and supervisory stress testing.
3. Emerging Digital Technologies and Privacy Concerns (Green cluster)
    a. Keywords such as "blockchain," "FinTech," "cloud computing," "Internet of Things," and "privacy" appear here, signaling an active stream of research exploring both the

opportunities and vulnerabilities posed by technological innovations in finance. It suggests the need for a balance between innovation incentives and data protection, interoperability, and coordination between the different sectors in cybersecurity.

The keyword frequency data reinforce this structure, with "cyber security" (550 occurrences), "information security" (202), "blockchain" (97), "machine learning" (93), "privacy" (59), "fintech" (59), and "phishing" (46) ranking among the most frequent terms in the dataset.

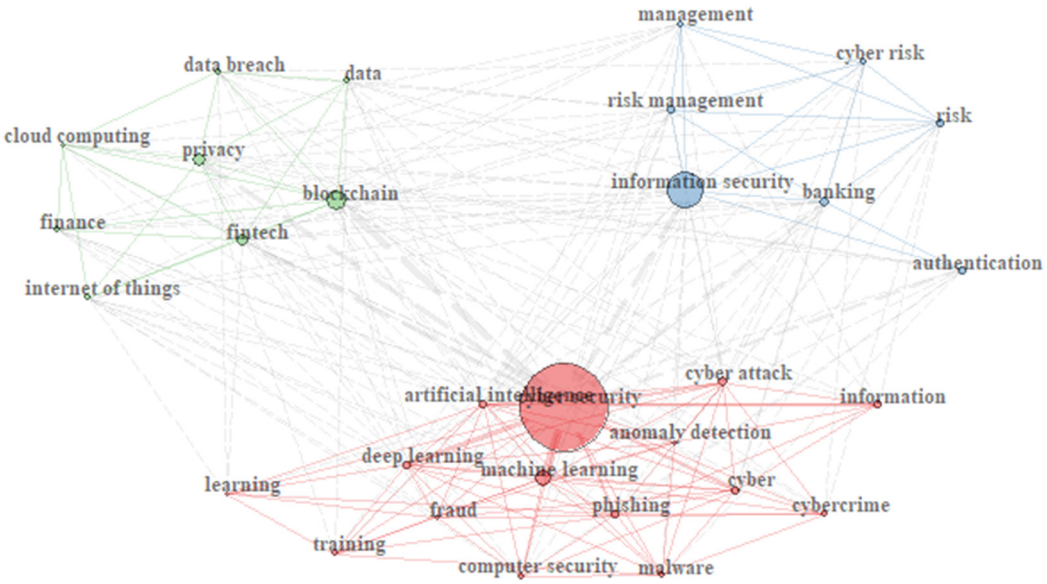

Figure 3. Keyword co-occurrence network diagram
Source: Own processing

The thematic evolution map (Figure 4) shows how these topics have shifted over time, segmented into three periods (RQ4): 2000–2015, 2016–2020, and 2021–2025. The first cut-off point (year 2015) precedes the 2016 Bangladesh Bank SWIFT cyber heist (Maurer & Nelson, 2021), which marked a turning point in industry awareness of systemic financial cyber threats. Early themes (during the period 2000–2015), such as "internet banking," "integrity," and "cyber security," gave way in 2016–2020 to more specialized topics, including "biometric authentication," "information security culture," "machine learning," and "malware." The second break (year 2020) aligns with the COVID-19 pandemic, which accelerated digital transformation and remote financial services, pushing "cyber risk," "cybersecurity," and "security" to prominence in the 2021–2025 period. This evolution highlights a sector-wide shift from foundational security measures to advanced, AI-supported risk mitigation and resilience strategies. The thematic mapping results (Figure 5) classify "privacy" as a motor theme, suggesting that it is both central and well-developed; "security" as a basic theme, indicating foundational relevance; "risk" as a niche theme, associated with specialized but significant inquiry; and "algorithm" in the emerging/declining quadrant, highlighting a need for renewed exploration of AI governance and resilience.

Table 3 lists the most locally cited articles within the dataset, highlighting those that have exerted a disproportionate influence on the research field (RQ3). Biener et al. (2015), examining the insurability of cyber risk, led with 29 local citations, framing much of the debate around financial risk transfer and resilience.

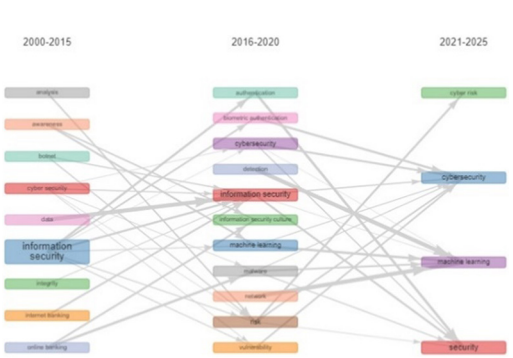

Figure 4. Thematic evolution map
Source: Own processing

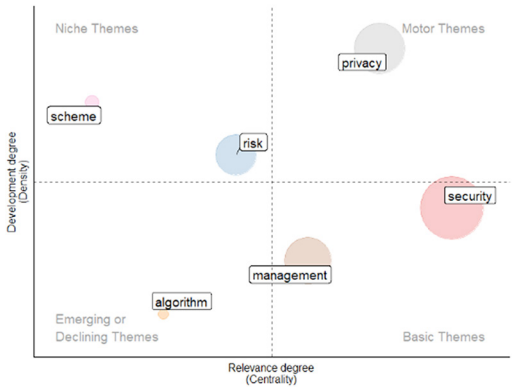

Figure 5. Thematic Keywords Plus map
Source: Own processing

Table 3. Co-citation analysis

Authors & Year	Topic	Cit.
Biener et al. (2015)	Insurability of cyber risk: An empirical analysis.	29
Davis (1989)	Perceived usefulness, perceived ease of use, and user acceptance of information technology	29
Gordon & Loeb (2002)	The economics of information security investment	23
Herath & Rao (2009)	Protection motivation and deterrence: a framework for security policy compliance in organizations	22
Cavusoglu et al. (2004)	The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers	19
Kamiya et al. (2021)	Risk management, firm reputation, and the impact of successful cyberattacks on target firms.	19

Source: Own processing

Gordon and Loeb (2002), with 23 citations, provide a foundational economic model for evaluating investments in information security widely applied in banking and insurance contexts. Together with other studies, these references anchor economic, behavioral, and market-impact perspectives that the field repeatedly builds on.

5. FUTURE RESEARCH DIRECTIONS

The evolution of cybersecurity research in financial institutions, as mapped in this study, reveals several trajectories that warrant deeper exploration. Emerging technological, regulatory, and organizational developments are reshaping the security landscape, creating opportunities for multidisciplinary, empirically grounded inquiry. First, the continued integration of artificial intelligence (AI), machine learning, and deep learning into cyber defense systems opens new avenues for research. While recent work has demonstrated the potential of AI-driven anomaly detection and predictive modelling (Sethi et al., 2025; Woods & Böhme, 2021), further investigation into algorithmic transparency, model governance, and resilience against adversarial attacks in high-stakes financial contexts is needed. The interaction between AI-based security tools and evolving regulatory requirements remains a largely underexplored area. Second, the rapid adoption of blockchain, FinTech, and cloud computing in banking and insurance presents novel

vulnerabilities alongside efficiency gains (Brando et al., 2022; Elmahdy et al., 2025). Future research should examine the design of secure architecture for these technologies, particularly under cross-border operational frameworks, and assess their role in mitigating or exacerbating systemic risk. Third, the increasing salience of privacy as both a regulatory mandate and a competitive differentiator calls for studies that connect technical privacy-enhancing measures with compliance obligations under frameworks such as the GDPR and emerging data localization laws (OECD, 2022). Longitudinal research could evaluate how privacy practices influence customer trust, firm performance, and market stability. Fourth, cyber risk quantification and modelling remain critical challenges. Building on work linking cyber risk to financial risk-taking (Sulong et al., 2025) and economic loss estimates (Bouveret, 2018; International Monetary Fund, 2024), future studies should advance predictive models that integrate macro-financial indicators, interbank connectivity, and behavioural factors. Such models could inform regulatory stress testing and capital adequacy assessments for cyber resilience. Finally, governance and cross-sector coordination merit deeper empirical investigation. While governance mechanisms such as dedicated IT committees and Chief Risk Officers have been associated with better cybersecurity outcomes (Elsayed et al., 2024), the effectiveness of these structures in different regulatory and cultural environments remains unclear. Comparative international studies could illuminate best practices for aligning organizational governance with evolving cyber threat landscapes. By addressing these themes, future research can bridge the technical, economic, and policy dimensions of financial-sector cybersecurity, ensuring that research efforts keep pace with the sector's rapidly shifting risk environment.

6. CONCLUSION

This study applied PRISMA-based systematic mapping and bibliometric analysis to 2,005 publications on cybersecurity in financial institutions from 2000 to 2025. By combining structured literature screening with science mapping via the bibliometrix package, we identified influential journals, highly cited works, major thematic clusters, and evolving research trends. The findings reveal a diverse but interconnected research landscape with three primary thematic domains: (i) AI-driven threat detection and technological safeguards, (ii) governance and institutional risk management, and (iii) emerging digital technologies and privacy.

The analysis highlights the increasing academic and policy focus on cybersecurity as a systemic risk factor for the financial sector, particularly following major inflection points such as the 2016 Bangladesh Bank cyber heist and the 2020 COVID-19 pandemic. These events have shifted the research frontier toward integrating advanced technologies with regulatory frameworks, enhancing governance structures, and addressing privacy and data protection in a globalized, digitally dependent financial system.

From a practical perspective, this study contributes sector-specific evidence-based that can inform institutional strategy and policy design aimed at strengthening cyber resilience. The results are relevant to regulators seeking to design adaptive oversight mechanisms, financial institutions aiming to integrate cybersecurity into enterprise risk management, and technology providers developing sector-specific security solutions.

This study has several limitations that provide avenues for additional research. First, the analysis was restricted to publications indexed in the Web of Science Core Collection, potentially omitting relevant work from other databases. Second, the focus on English-language publications may introduce a language bias, underrepresenting perspectives from non-English-speaking regions.

Third, bibliometric methods privilege citation-based influence, which may not always correlate with practical impact or emerging niche research. Finally, the dataset reflects research activity up to mid-2025, meaning that very recent developments may not yet be fully represented in the available literature.

Despite these constraints, this study provides a transparent and replicable framework for understanding the intellectual and thematic structure of cybersecurity research in financial institutions. Mapping the evolution of the field and identifying thematic gaps offers both a consolidated reference for current research and a foundation for future inquiry.

Acknowledgment

This work was partially supported by the MINEDU of the Slovak Republic [grant No. 1/0638/25] and the Slovak Research and Development Agency under Contract no. VV-MVP-24-0272.

References

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector. *BIS Working Papers*, No 840.

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

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. *IMF Working Papers, 18*(143), 1. https://doi.org/10.5089/9781484360750.001

Bouyon, S., & Krause, S. (2018). *Cybersecurity in finance: Getting the policy mix right*. Rowman & Littlefield.

Brando, D., Kotidis, A., Kovner, A., Lee, M., & Schreft, S. L. (2022). Implications of Cyber Risk for Financial Stability. *FEDS Notes, 2022.0*(3077.0). https://doi.org/10.17016/2380-7172.3077

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

Cooper, C., Booth, A., Varley-Campbell, J., Britten, N., & Garside, R. (2018). Defining the process to literature searching in systematic reviews: a literature review of guidance and supporting studies. *BMC Medical Research Methodology*, *18*(1), 85. https://doi.org/10.1186/s12874-018-0545-3

Daimi, K., & Peoples, C. (Eds.). (2021). *Advances in Cybersecurity Management*. Springer. https://doi.org/10.1007/978-3-030-71381-2

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340. https://doi.org/10.2307/249008

Elmahdy, A. H. A. M., Abdelkader, M. T. K. M., & Shaker, M. A. M. (2025). Bridging the nexus between Fintech, operational efficiency and banks profitability: the moderating role of bank size. *Future Business Journal*, *11*(1). https://doi.org/10.1186/s43093-025-00478-x

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal*, *10*(1). https://doi.org/10.1186/s43093-024-00402-9

Galletta, S., Mazzù, S., Naciti, V., & Paltrinieri, A. (2024). A PRISMA systematic review of greenwashing in the banking industry: A call for action. *Research in International Business and Finance*, *69*, 102262. https://doi.org/10.1016/j.ribaf.2024.102262

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *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

International Monetary Fund. (2024). *Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks*. Washington, DC, April. https://doi.org/10.5089/9798400257704.082

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, *37*(4), 480-501. https://doi.org/10.1177/1043986211027986

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gotzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions: explanation and elaboration. *BMJ, 339*(jul21 1), b2700-b2700. https://doi.org/10.1136/bmj.b2700

Makarenko, E. N., Vovchenko, N. G., & Tishchenko, E. N. (2023). *Technological Trends in the AI Economy. Smart Innovation, Systems and Technologies.* Springer Nature. https://doi.org/10.1007/978-981-19-7411-3

Maurer, T., & Nelson, A. (2021). The global cyber threat. *Finance & Development*, *58*(1), 24-27.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & the PRISMA Group*. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Annals of Internal Medicine, 151*(4), 264-269. https://doi.org/10.7326/0003-4819-151-4-200908180-00135

Nelson, A., & Wang, S. (2024). The importance of cybersecurity disclosures in customer relationships. *Journal of Corporate Accounting & Finance*, *35*(3), 66-74. https://doi.org/10.1002/jcaf.22695

OECD. (2022). *OECD Policy Framework on Digital Security*, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en

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., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Pendley, J. A. (2018). Finance and accounting professionals and cybersecurity awareness. *Journal of Corporate Accounting & Finance*, *29*(1), 53-58. https://doi.org/10.1002/jcaf.22291

Prodan, S., Konhäusner, P., Dabija, D.-C., Lazaroiu, G., & Marincean, L. (2024). The rise in popularity of central bank digital currencies. A systematic review. *Heliyon*, *10*(9), e30561. https://doi.org/10.1016/j.heliyon.2024.e30561

Ravikumar, R. (2025). Strengthening Cybersecurity: Lessons from the Cybersecurity Survey. *Technical Notes and Manuals, 2025*(006), 1. https://doi.org/10.5089/9798400296864.005

Sethi, M., Bohra, N. S., Johri, A., & Asif, M. (2025). Emerging dimensions in Fintech: Insights from bibliometric analysis. *Digital Business*, *5*(1), 100113. https://doi.org/10.1016/j.digbus.2025.100113

Sulong, Z., Fuszder, M. H. R., Abdullah, M., & Abakah, E. J. A. (2025). Cybersecurity risk and bank risk-taking. *Journal of Behavioral and Experimental Finance*, 101080. https://doi.org/10.1016/j.jbef.2025.101080

Taplin, R. (Ed.). (2016). *Managing Cyber Risk in the Financial Sector*. Routledge, Taylor & Francis Group. https://doi.org/10.4324/9781315675930

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, *14*(3), 207-222. https://doi.org/10.1111/1467-8551.00375

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