DOI: 10.20472/EFC.2025.026.011

JAKUB SOPKO
Faculty of Economics, Technical University of Košice, Slovakia
LEOŠ ŠAFÁR
Faculty of Economics, Technical University of Košice, Slovakia

MAPPING CYBERSECURITY RESEARCH IN FINANCIAL AND ECONOMIC CONTEXTS: TRENDS, KEY CONTRIBUTORS, AND EMERGING THEMES

Abstract:

This study conducts a bibliometric analysis to map the intellectual structure and thematic evolution of cybersecurity research in financial and economic contexts from 2000 to June 2025. Using 866 articles and conference proceedings retrieved from the Web of Science Core Collection, the analysis combines descriptive performance indicators with co-citation and co-occurrence network techniques to examine publication trends, leading contributors, and emerging research streams.

The results show a steady increase in publication activity, with a significant surge after 2017 driven by regulatory initiatives, high-profile cyber incidents, and rapid digitalization in the financial sector. A highly concentrated productivity pattern is evident, with a small group of influential scholars contributing disproportionately to the field. Leading journals, such as Computers & Security and Journal of Operational Risk, indicate the interdisciplinary nature of the research, integrating technical, financial, and governance perspectives.

Thematic network analysis reveals a shift from fragmented technical or behavioral studies toward integrated research streams, where artificial intelligence, fintech, systemic governance, and risk management converge. This transition highlights the growing focus on financial system resilience, risk transfer mechanisms, and strategic investment in cybersecurity. The study provides a structured overview of the field's development and identifies research gaps to guide future work on managing systemic cyber risks in financial systems.

Keywords:

Cybersecurity, Fintech, Bibliometric analysis, Financial institutions, Cyberattack

JEL Classification: G20, G21, M15

1 INTRODUCTION

The accelerating digital transformation of financial and industrial systems has fundamentally reshaped the nature of operational risk. Industry 4.0 and interconnected cyber-physical infrastructures significantly increase efficiency and innovation but simultaneously expose organizations to sophisticated cyber threats with potentially systemic implications (Bouveret, 2018). Recent evidence highlights that cyberattacks on financial and critical infrastructures have increased in frequency and severity, with the financial sector being among the most targeted due to its reliance on sensitive data and real-time transactions (Wang et al., 2024). High-profile incidents, such as the Bangladesh Bank SWIFT breach and large-scale ransomware campaigns, demonstrate the potential for cascading disruptions and reputational losses across entire supply chains (Uddin et al., 2020).

The economic consequences of cyber incidents extend beyond immediate remediation costs. Studies have shown substantial indirect losses, including market valuation declines, reputational damage, and increased financing costs (Brho et al., 2025). Despite growing investments in cybersecurity, the financial efficiency of these expenditures remains debated. Some authors argue that cybersecurity spending may be overestimated due to inadequate financial modeling and limited incorporation of tax, leverage, and cost-of-capital considerations (Chong et al., 2025; Brho et al., 2025). Others emphasize that governance, interorganizational collaboration, and resilience-based approaches are equally critical for mitigating cyber risk (Tagarev et al., 2022).

Given these challenges, assessing cybersecurity investment and governance strategies is crucial for ensuring resilience, especially in highly digitalized financial ecosystems. However, the literature remains fragmented, with limited integration of financial, technical, and governance perspectives, which this paper aims to address.

The aim of this paper is to systematically map the development of cybersecurity research in financial and economic contexts via a bibliometric analysis of publications from 2000 to June 2025. This study seeks to uncover the intellectual structure, identify influential contributions, and highlight underexplored directions in the field. To achieve this aim, this study addresses the following research questions: (R1) How has the volume and thematic focus of cybersecurity research evolved between 2000 and June 2025? (R2) Which authors, institutions, and publications have shaped the intellectual development of this field? (R3) What are the dominant research streams, and how are they interconnected? (R4) Which emerging topics and knowledge gaps can be identified for future research and policy-making?

By answering these questions, this paper aims to provide an evidence-based overview of the evolution of cybersecurity research and to guide both scholars and practitioners toward more integrated and strategic approaches to cyber risk management.

2 LITERATURE REVIEW

The body of literature on cybersecurity in financial institutions reflects an evolving yet fragmented understanding of risks, investment efficiency, and governance. The integration of Industry 4.0 technologies, while improving efficiency, increases attack surfaces, requiring resilience-based approaches. Kosmowski (2023) highlighted the need to combine functional safety and cybersecurity in operational resilience frameworks for industrial control systems. This aligns with broader arguments that resilience, rather than prevention alone, should be the primary strategic objective in managing cyber risk. Early actuarial studies quantified cyber losses through

probabilistic modeling, with Eling and Wirfs (2019) classifying risks by cause and Eling and Jung (2018) analyzing dependencies in data breach events via vine copulas. Xu et al. (2018) identified temporal trends in hacking incidents, whereas Kamiya et al. (2021) demonstrated that governance features, such as the presence of risk oversight committees, influence both the frequency and severity of losses. Eisenbach et al. (2022) highlighted the systemic nature of cyber threats by showing how incidents can propagate through payment systems, amplifying financial contagion. In addition to loss modeling, economic studies have explored optimal investment strategies. Gordon and Loeb (2002) proposed balancing the marginal costs of cybersecurity spending against expected reductions in loss probabilities, whereas Smeraldi and Malacaria (2014) applied a knapsack optimization framework to allocate limited security budgets across multiple assets. The literature also draws analogies to the Laffer curve, emphasizing trade-offs between immediate cybersecurity spending and the long-term capital needed to absorb residual risk. Recent research increasingly recognizes that overinvestment may diminish returns and even escalate operational risk, as noted by Uddin et al. (2020), who argue that excessive reliance on cyber technologies can undermine financial stability.

Despite these advances, significant gaps persist. Woods and Böhme (2021) stress the need for causal models that account for latent variables such as threat exposure and organizational maturity to evaluate the effectiveness of security interventions. Similarly, Domínguez-Dorado et al. (2021) call for scalable tactical-operational frameworks, such as CyberTOMP, to bridge governance and technical layers in financial institutions. Theoretical models often lack actionable asset-level guidance, whereas cost–benefit analyses remain underutilized in organizational practice, as observed by Alahmari and Duncan (2020). Moreover, as highlighted by Tagarev et al. (2021), cross-sectoral collaboration and skill-building initiatives are critical yet underexplored in the financial sector. Cybersecurity in financial institutions is increasingly viewed as a systemic risk factor, as cyber incidents can propagate through interconnected markets, affecting liquidity, stability, and customer trust (Bouveret, 2018). Quantitative frameworks, such as value-at-risk (VaR) and return-on-security-investment (ROSI), have been applied to estimate potential financial losses, but empirical evidence remains scarce and often limited to operational cost data (Barcellos-Paula et al., 2025). Moreover, stock market event studies consistently demonstrate significant abnormal returns following cyber breaches, underscoring the reputational dimension of cyber risk (Brho et al., 2025). The distinction between capital (investment) and operational (spending) expenditures is critical but often overlooked in cybersecurity financial assessments. Brho et al. (2025) propose the Alpha Model, which integrates financial parameters such as the cost of capital, leverage, and tax credits to compute the net present value of cybersecurity investments. Their findings suggest that the true economic value of cybersecurity investments is often substantially lower than their book value, challenging traditional cost–benefit analyses.

Collectively, the literature underscores the urgency of integrating economic modeling, governance mechanisms, and resilience-based approaches to manage increasingly complex cyber risks.

3 DATA AND METHODOLOGY

This study employs bibliometric analysis (Aria & Cuccurullo, 2017) to systematically map the intellectual structure and thematic evolution of cybersecurity research in the financial and economic domains. Bibliometric methods are widely recognized for their ability to identify trends, influential contributions, and emerging topics within a research field over time. The methodological framework is designed to address the following research questions:

- R1: How has the volume and thematic focus of cybersecurity research evolved between 2000 and June 2025?
- R2: Which authors, institutions, and publications have shaped the intellectual development of this field?
- R3: What are the dominant research streams, and how are they interconnected?
- R4: Which emerging topics and knowledge gaps can be identified for future research and policy-making?

A quantitative science mapping approach will be applied, combining descriptive performance analysis (publication and citation trends, leading authors, and institutions) and science mapping techniques (co-word, co-citation, and thematic network analysis) to provide a comprehensive understanding of the field.

The bibliometric data were downloaded from the Web of Science (WoS) Core Collection, ensuring a high level of quality and standardized indexing. The search strategy was defined to capture research focusing on cybersecurity and its implications in the financial sector, using carefully selected keywords (Table 1).

Table 1 Descriptive analysis of the dataset

Search timeframe	**2000 – June 2025**
Document types	Journal articles, conference proceedings
Language	English
Fields	Topic (TS) – titles, abstracts, author keywords, Keywords Plus
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

Table 1 presents a descriptive overview of the dataset search strategy. The search was restricted to articles and conference proceedings published in English from 2000 to June 2025. The Topic (TS) field was used, which queries titles, abstracts, author keywords, and Keywords Plus. Thematic areas were grouped into Cybersecurity (e.g., “cybersecurity”, “cyber risk”, “cyber-attack”, “data breach”, “IT security”) and Financial sector (e.g., “bank*”, “financial institution*”, “fintech”, “financial service*”, “insurance”). The initial search yielded 32,436 records related to cybersecurity keywords and 111,344 records related to financial and banking keywords. To focus the dataset on the intersection of these two thematic areas, an iterative filtering process was conducted, as outlined in the PRISMA flowchart (Figure 1).

The selection process followed PRISMA guidelines to ensure transparency and replicability. In the “identification stage”, a total of 1,336 records were retrieved after the two thematic areas were combined and duplicates were removed. Only journal articles and conference proceedings were retained, excluding review papers, early access, book chapters, editorials, and other nonresearch outputs (n = 100 excluded; remaining = 1,236) in the first stage of the “screening process”.

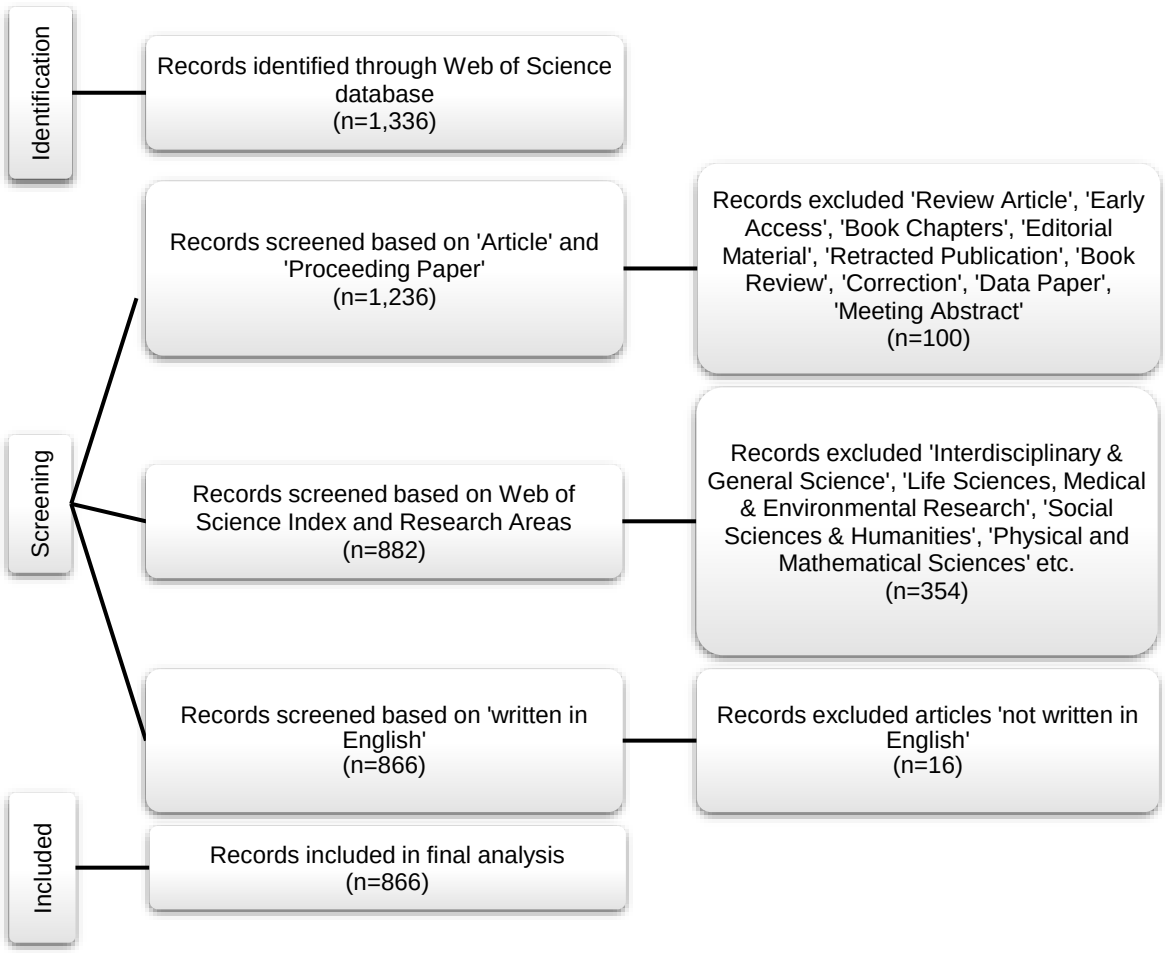


Figure 1 PRISMA flowchart

Source: prepared by the authors

In the second stage of the “screening process”, records not associated with business, finance, economics, management, or relevant governance fields were excluded. Categories such as interdisciplinary general science, life sciences, medical and environmental research, social sciences & humanities, and physical and mathematical sciences were removed (n = 354 excluded; remaining = 882). Non-English publications were also excluded (n = 16 excluded). Finally, 866 records met all the criteria and were included in the bibliometric analysis.

The final dataset (Table 2) covers publications from 2001 to 2025, as no eligible studies were published in 2000. It comprises 866 documents, including 467 journal articles and 395 conference proceedings papers. Four records were classified simultaneously as articles and proceedings papers by WoS. These documents are distributed across 629 sources (journals, books, and proceedings) and authored by 2,636 unique authors. In terms of bibliometric indicators, the dataset contains 2,927 author keywords (DE) and 682 Keywords Plus (ID), with an average of 11.08 citations per document, indicating a moderate but growing academic impact.

Table 2 Final dataset

Description	Results
Documents	866

Period	2001-2025
Sources (Journals, Books, etc.)	629
Keywords Plus (ID)	682
Author's Keywords (DE)	2927
Average citations per doc	11.08
Authors	2636
Article	467
Article; Proceedings Paper	4
Proceedings Paper	395

Source: prepared by the authors

The analysis was conducted via RStudio with the Bibliometrix package (Aria & Cuccurullo, 2017). Publication and citation trends were assessed to address R1, whereas leading authors, institutions, and journals were identified to address R2. In the next phase of the methodology approach (R3-R4), we applied the co-citation analysis to detect intellectual clusters, and co-word analysis based on the authors' keywords (DE) and keywords plus (ID) was used to map thematic networks and track the evolution of research streams over the study period.

4 RESULTS & DISCUSSION

The scientific output on cybersecurity in financial and economic contexts clearly has increased over the past two decades (Figure 2). Between 2001 and 2010, publication activity was minimal, reflecting a limited academic focus on financial cyber risk during the early stages of digital banking. A gradual rise began after 2011, driven by the expansion of online financial services and increasing regulatory attention.

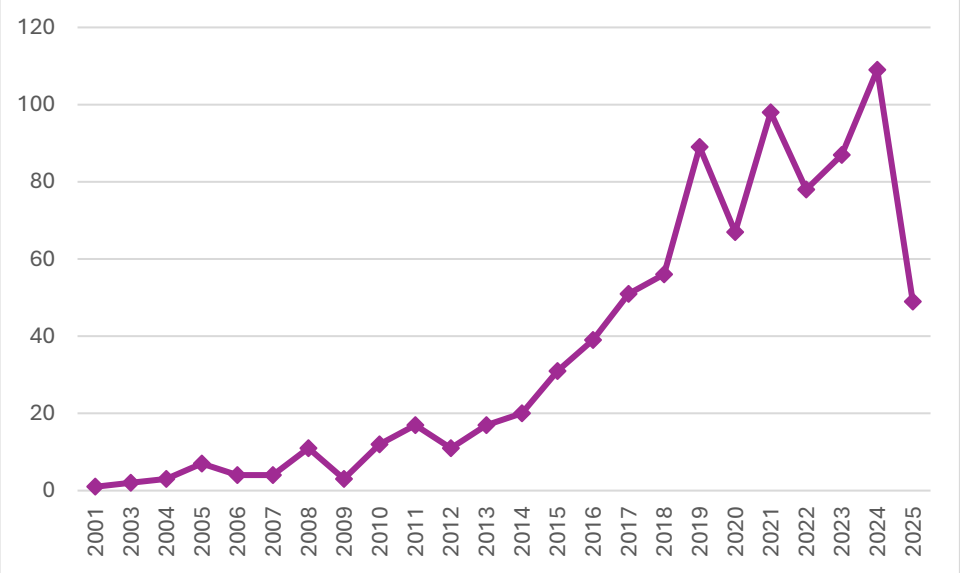


Figure 2 Number of publications from 2001 to 2025

Source: prepared by the authors

A sharp growth phase is observed from 2017 to 2019, with outputs exceeding 50 publications annually, coinciding with high-profile incidents (e.g., SWIFT attacks (Uddin et al., 2020)) and regulatory measures such as the GDPR (Lessa & Gebrehawariat, 2023). The field reached its

highest level of activity between 2020 and 2023 (80–110 publications annually), likely due to heightened cybersecurity concerns during the COVID-19 digitalization surge and growing interest in systemic financial stability and resilience (Georgiadou et al., 2022). Overall, the trend confirms that cybersecurity in financial institutions has evolved into a mature interdisciplinary field, increasingly engaging finance, economics, and management scholars alongside computer scientists.

4.1 The most productive countries and top contributing authors

Table 3 reveals that research on cybersecurity in financial contexts is globally diverse but dominated by a few countries. The United States (U.S.) leads with 136 publications (16% of total output), reflecting its strong research base and policy interest in financial cyber resilience. The SCP/MCP ratio (0.176) indicates that the U.S. produces primarily single-country publications (SCPs), suggesting a strong national research base with comparatively limited international collaboration. India (n = 84; 9.9%) and China (n = 58; 6.8%) followed, driven by the rapid expansion of fintech ecosystems and growing systemic risk awareness in emerging economies. The relatively low MCP ratios (India = 0.07; China = 0.17) also indicate a predominance of domestic collaboration.

Table 3 Most productive countries

Country	Articles	Freq	Single country publication	Multiple country publication	MCP_Ratio
USA	136	0.16	112	24	0.1765
INDIA	84	0.0988	78	6	0.0714
CHINA	58	0.0682	48	10	0.1724
UNITED KINGDOM	41	0.0482	27	14	0.3415
AUSTRALIA	28	0.0329	19	9	0.3214
RUSSIA	28	0.0329	25	3	0.1071
SOUTH AFRICA	28	0.0329	25	3	0.1071
KOREA	27	0.0318	22	5	0.1852
ITALY	23	0.0271	19	4	0.1739
MALAYSIA	21	0.0247	13	8	0.381

Source: prepared by the authors

Table 4 highlights the most productive and influential authors. The table is divided into two parts: the left presents raw productivity (articles and total citations), whereas the right shows fractionalized article counts, which adjust for co-authorship by distributing credit proportionally. Gupta M leads with four publications, followed by a group of scholars with three publications each, including Aldasoro I, Asif M, and Dhillon G. In terms of influence, Gai K stands out with 386 citations, indicating substantial impact, possibly due to highly cited foundational work on cybersecurity in financial technologies.

Table 4 The top contributing authors

Authors	Articles	Total citations	Authors	Articles Fractionalized
GUPTA M	4	64	IFINEDO P	3
ALDASORO I	3	52	TROMMLER P	2
ASIF M	3	56	DHILLON G	1.83
AXON L	3	6	CHOI Y	1.67
CREESE S	3	6	GORIAN E	1.5
DHILLON G	3	84	LUBURIC R	1.5
EROLA A	3	6	MOECKEL C	1.5

FEDOTOVA GV	3	4	NAGURNEY A	1.5
GAI K	3	386	ORLANDO A	1.5
GAMBACORTA L	3	52	STEWART H	1.5

Source: prepared by the authors

The right part highlights Ifinedo P as the top contributor with 3 fractionalized articles, indicating strong individual involvement, likely as the primary or sole author. In other words, his contribution across papers is equivalent to approximately 3 full single-author articles. Dhillon G shows 1.83 fractionalized articles, suggesting more collaborative works. This comparison reveals that some authors (e.g., Gai K) are highly cited across broader collaborations, whereas others (e.g., Ifinedo P) contribute more intensively to fewer studies, underscoring the collaborative yet specialized nature of the field.

Lotka's Law (Aria & Cuccurullo, 2017) analysis revealed that 93.7% of the authors published only one article, whereas a small group of highly productive scholars contributed multiple papers. The beta coefficient (β = 5.24), which is greater than the classical value (~2), indicates a greater concentration of productivity, which is typical for emerging interdisciplinary fields. The goodness-of-fit (R^2 = 0.94) and nonsignificant Kolmogorov–Smirnov test (p = 0.21) imply that the observed distribution does not significantly differ from Lotka's theoretical distribution.

4.2 Publication distribution by source type

Among the sources (Table 5), IEEE Access leads in productivity (30 articles, m-index = 1.33), whereas Computers & Security demonstrates the greatest influence (22 articles, Total Citations (TC) = 993, g-index = 22), reflecting its long-standing relevance. Information and Computer Security and Expert Systems with Applications contribute significantly to technical and applied aspects, whereas journals such as the Journal of Operational Risk and Risks highlight the growing integration of cyber risk into financial risk management. The mix of technical and risk-focused outlets underscores the interdisciplinary character of the field.

Table 5 Leading sources

Sources	Articles	TC	h_index	g_index	m_index	PY_start
IEEE Access	30	363	12	18	1.333333	2017
Computers \\& Security	22	993	14	22	0.56	2001
Information and Computer Security	18	353	10	18	0.909091	2015
International Journal of Advanced Computer Science and Applications	8	13	2	3	0.133333	2011
International Journal of Security and its Applications	8	20	3	4	0.1875	2010
Journal of Operational Risk	7	20	3	4	0.375	2018
Risks	7	32	3	5	0.5	2020
Decision Support Systems	5	211	5	5	0.238095	2005
Expert Systems with Applications	5	364	5	5	0.357143	2012
Financial and Credit Activity-Problems of Theory and Practice	5	5	2	2	0.4	2021

Source: prepared by the authors

The impact of a journal can be evaluated via several citation-based indicators. The h-index represents the number of articles (h) that have each received at least h citations, providing a balanced measure of productivity and citation impact. The g-index, which gives greater weight to highly cited papers, is defined as the largest number (g) such that the top g articles collectively

have at least g² citations, thus emphasizing journals with highly influential publications. The m-index refines the h-index by normalizing it to the journal's active publication years in the field, allowing for a fair comparison between newer and more established journals.

4.3 Co-citation network

Table 6 highlights the most influential works within the dataset on the basis of local citation counts. The analysis complements the earlier findings on productivity and leading sources, reinforcing the interdisciplinary and evolving nature of the field. While Lotka's Law indicates that most authors contribute only once, the presence of influential works by a small core group (e.g., Gordon & Loeb, 2002; Biener et al., 2015) aligns with the highly concentrated productivity pattern (β = 5.24). These foundational studies bridge economic modeling, insurance risk assessment, and market impact analysis, directly supporting the trends observed in leading outlets such as Computers & Security and the Journal of Operational Risk, which specialize in the technical and financial aspects of cyber risk.

Table 6 Top locally cited authors

Authors & Year	Topic	Citations
Biener, C., Eling, M., & Wirfs, J. H. (2015)	Insurability of cyber risk: An empirical analysis.	20
Davis, F. D. (1989)	Perceived usefulness, perceived ease of use, and user acceptance of information technology	17
Fornell, C., & Larcker, D. F. (1981)	Evaluating structural equation models with unobservable variables and measurement error	16
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	14
Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2017)	A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)	14
Gordon, L. A., & Loeb, M. P. (2002)	The economics of information security investment	12

Source: prepared by the authors

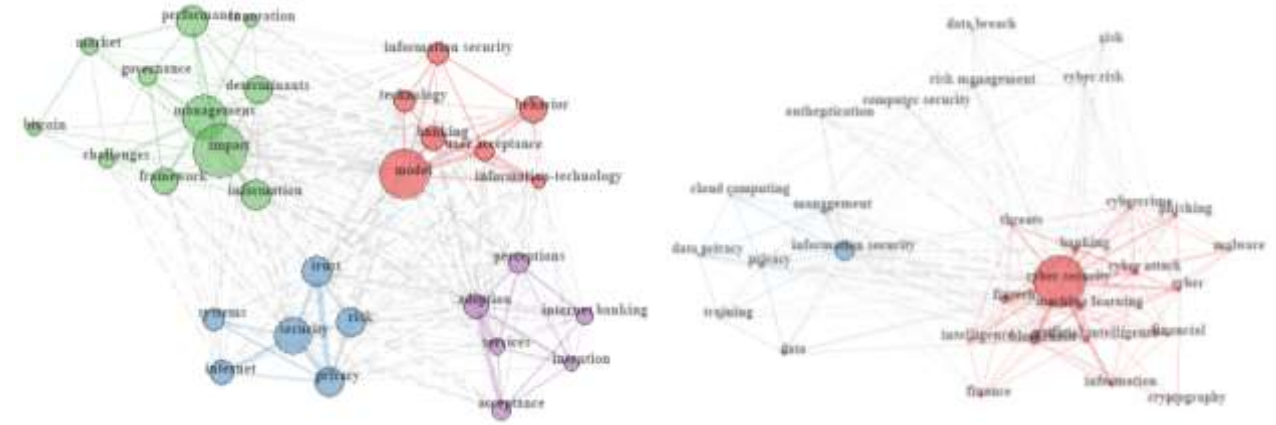
Similarly, the high number of local citations of methodological works (e.g., Fornell & Larcker, 1981; Hair et al., 2017) reflects the growing reliance on robust statistical and behavioral modeling methods, which is consistent with the shift in recent years toward systemic risk evaluation and user behavior analysis (as discussed in the thematic evolution of publications). This interplay between core theoretical contributions and rising publication output in applied risk-focused journals confirms that the field is transitioning from isolated technical studies to a more integrated, finance-oriented research agenda.

4.4 Co-occurrence network

The Authors' Keyword Co-occurrence Network (Figure 3, right side) highlights research trends as perceived by the authors themselves. After the synonyms (e.g., "cybersecurity; cyber security; cyber-security") are harmonized, several distinct thematic clusters emerge. The largest red cluster centers on "cybersecurity," "banking," "machine learning," and "cyber attack," emphasizing technical and financial risk mitigation approaches, including fintech and AI applications. The blue cluster is related to "information security," "data privacy," and "cloud computing," suggesting

organizational and privacy-focused concerns, whereas the smaller green cluster focuses on “risk management” and “data breach.”

The Keywords Plus Co-occurrence Network (Figure 3, left side), derived from cited references, reflects broader conceptual structures. Here, the clusters emphasize governance and market performance (green), technology adoption and user acceptance (purple), and trust, privacy, and security frameworks (blue), alongside information security and behavioral aspects (red). Compared with authors’ keywords, Keywords Plus reveals a stronger conceptual and behavioral orientation, highlighting systemic governance, market implications, and user behavior models. Keywords-Plus are automatically generated by Web of Science on the basis of the titles of the references cited by the authors, thereby capturing the underlying intellectual structure and contextual background of the research. In summary, authors’ keywords capture current, application-oriented research trends, whereas Keywords Plus maps the underlying conceptual and methodological foundations of the field, confirming its interdisciplinary nature.



Keywords plus co-occurrence analysis | Authors’ keyword co-occurrence analysis

Figure 3 Co-occurrence network analysis

Source: prepared by the authors

The co-occurrence network analysis confirms and extends the patterns discussed in the previous sections, illustrating how the field of cybersecurity in financial contexts is evolving toward greater interdisciplinarity. The authors’ keyword network, where “cybersecurity,” “banking,” “fintech,” “machine learning,” and “cyber attack” form the dominant cluster, aligns with findings in Biener et al. (2015) and Gordon & Loeb (2002), which stressed the need for optimal investment strategies in cyber protection for financial institutions. The strong association between machine learning and fintech indicates a growing transition toward technology-enhanced risk assessment and automation, a trend also highlighted in Eling & Wirfs (2019), Uddin et al. (2020), and Wang et al. (2024), which pointed to AI as a key driver for improving cyber resilience in financial systems. The privacy and information security clusters (blue cluster) resonate with the behavioral and governance issues discussed by Uddin et al. (2020), who emphasized that cybersecurity vulnerabilities in financial systems are often exacerbated by human and organizational factors. The presence of “data privacy,” “cloud computing,” and “management” keywords reflects the organizational governance and training aspects stressed in Tagarev et al. (2022), who argued that strengthening human and managerial capacities is a core element of cyber resilience.

The Keywords Plus network, which highlights “governance,” “frameworks,” “market performance,” and “risk management,” reinforces the systemic perspective advanced by Domínguez-Dorado et al. (2022) and Woods & Böhme (2021). Domínguez-Dorado et al. (2022) emphasized the need for tactical-operational frameworks linking governance with technical controls, whereas Woods & Böhme (2021) called for causal models connecting organizational maturity with systemic financial risk. Our network confirms that such governance and systemic risk topics are now thematically central, as they co-occur with terms such as “finance,” “cryptography,” and “artificial intelligence,” bridging financial stability and technological security research.

Finally, the identification of risk and market-related clusters corresponds with Cavusoglu et al. (2004), who demonstrated the financial market impact of cyber breaches, and with Biener et al. (2015), whose work on cyber-risk insurability is reflected in the growing attention to risk transfer and resilience in systemic finance. This convergence of economic, behavioral, and technical themes across the co-occurrence networks suggests that the field is shifting from isolated studies to an integrated research agenda, where technical innovation, governance, and financial systemic stability are increasingly intertwined.

5 CONCLUSIONS

This study systematically examined the evolution of cybersecurity research in financial and economic contexts between 2000 and June 2025, revealing important developments in its intellectual and thematic structure. The results show a clear upward trend in publication activity, with a sharp increase after 2017 triggered by high-profile cyber incidents, regulatory initiatives such as the GDPR, and the rapid digitalization of financial services during the COVID-19 period. These findings confirm earlier observations by Uddin et al. (2020) and Wang et al. (2024), who highlighted the growing systemic vulnerabilities associated with digital transformation in the financial sector.

The analysis of authors, institutions, and countries confirms a highly concentrated productivity pattern, which is consistent with Lotka’s Law, where a small core group of scholars plays a central role in shaping the field. Authors such as Gai K, Dhillon G, and Ifinedo P have made substantial contributions, either through highly cited collaborative works or strong individual involvement. Journals including Computers & Security and the Journal of Operational Risk dominate the field, reflecting its interdisciplinary nature by combining technical innovations with financial risk management approaches, as emphasized in the works of Eling and Wirfs (2019) and Gordon and Loeb (2002). The co-citation and co-occurrence network analyses reveal that the field is gradually shifting from fragmented technical or behavioral studies to integrated research streams, where artificial intelligence, fintech applications, risk transfer mechanisms, and systemic governance increasingly intersect. This development supports the systemic risk perspective described by Woods and Böhme (2021) and aligns with the tactical-operational frameworks proposed in Domínguez-Dorado et al. (2022). The emergence of governance, privacy, and organizational themes also reflects the growing relevance of human and managerial factors, echoing the conclusions of Tagarev et al. (2022).

Overall, the field is moving toward a holistic research agenda that integrates technical innovation, governance structures, and economic modeling to address the complex nature of cyber risk in financial systems. This interdisciplinary approach is essential for improving financial system resilience, supporting more efficient investment decisions, and reducing systemic vulnerabilities in the face of increasingly sophisticated cyber threats.

Acknowledgements

This paper was supported by the MINEDU of the Slovak Republic as part of the research project VEGA 1/0638/25 “Financial system vulnerability in the context of cybersecurity risk”.

6 References

Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1-5). IEEE.

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of informetrics*, *11*(4), 959-975.

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.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

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.

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.

Chong, W. F., Feng, R., Hu, H., & Zhang, L. (2025). Cyber risk assessment for capital management. *Journal of Risk and Insurance*, *92*(2), 424-471.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Domínguez-Dorado, M., Carmona-Murillo, J., Cortés-Polo, D., & Rodríguez-Pérez, F. J. (2022). CyberTOMP: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels. *IEEE Access*, *10*, 122454-122485. https://doi.org/10.1109/ACCESS.2022.3223440

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics*, *145*(3), 802-826.

Eling, M., & Jung, K. (2018). Copula approaches for modeling cross-sectional dependence of data breach losses. *Insurance: Mathematics and Economics*, *82*, 167-180.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events?. *European Journal of Operational Research*, *272*(3), 1109-1119.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *35*(2), 486-505.

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.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2017) A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). 2nd Edition, Sage Publications Inc., Thousand Oaks, CA.

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.

Kosmowski, K. T. (2023). Operational resilience regarding safety and security aspects of industrial automation and control systems. *Safety and Reliability of Systems and Processes*.

Lessa, L., & Gebrehawariat, D. (2023). Effectiveness of banking card security in the Ethiopian financial sector: PCI-DSS security standard as a lens. *International Journal of Industrial Engineering and Operations Management*, *5*(2), 135-147.

Smeraldi, F., & Malacaria, P. (2014, May). How to spend it: optimal investment for cyber security. In *Proceedings of the 1st International Workshop on Agents and CyberSecurity* (pp. 1-4).

Tagarev, T., Davis, B. A., & Cooke, M. (2022). Business, Organisational and governance modalities of collaborative cybersecurity networks. Multimedia Tools and Applications, 81(7), 9431-9443.

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.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & security*, *147*, 104051.

Woods, D. W., & Böhme, R. (2021, May). 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

Xu, M., Schweitzer, K. M., Bateman, R. M., & Xu, S. (2018). Modeling and predicting cyber hacking breaches. *IEEE Transactions on Information Forensics and Security*, *13*(11), 2856-2871.