South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Banking on resilience: 20 years of cybersecurity evolution

Authors:
Ntokozo F. Miya[1]
Nazeer Joseph[1]

Affiliations:
[1]Department of Applied Information Systems, College of Business and Economics, University of Johannesburg, Johannesburg, South Africa

Corresponding author:
Nazeer Joseph,
njoseph@uj.ac.za

Dates:
Received: 14 Apr. 2025
Accepted: 28 July 2025
Published: 18 Sept. 2025

How to cite this article:
Miya, N.F. & Joseph, N., 2025, 'Banking on resilience: 20 years of cybersecurity evolution', *South African Journal of Information Management* 27(1), a2019. https://doi.org/10.4102/sajim.v27i1.2019

Background: The rise in cyberattacks, particularly targeting financial institutions, poses significant risks. A shift towards cyber threat resilience, emphasising proactive strategies for recovery and adaptation, is essential. The financial sector must develop and implement holistic resilience strategies to ensure long-term operational preparedness against evolving cyber threats.

Objectives: The objectives of this bibliometric analysis were twofold. Firstly, to identify trends, patterns, and relationships in the literature on information system (IS) cyber resilience in the financial sector. Secondly, to explore how research on IS resilience has evolved and to identify key themes and emerging topics in the field.

Method: The study retrieved 228 documents from the Scopus database. Analysis techniques included citation analysis, coauthorship analysis, co-word analysis, and network analysis. The analysis was performed using Biblioshiny.

Results: The results reveal a significant uptick in 2018. Collaboration patterns support steady growth, but many developing nations are underrepresented. The study indicates a link between risk management and cybersecurity in the finance sector and supports the drive to develop resilience strategies and frameworks. Existing literature has primarily focused on cybersecurity measures and technical defences without sufficient attention to how organisations recover and maintain operations after a cyberattack. There is insufficient focus on enabling shared resilience cultures, as organisational preparedness goes beyond technology.

Conclusion: The bibliometric analysis highlights gaps in cybersecurity literature, emphasising the need for integrated frameworks, proactive strategies, and cross-disciplinary collaboration to enhance cyber threat resilience and preparedness.

Contribution: The study highlights the fragmented nature of cyber threat resilience literature in the financial sector.

Keywords: cybersecurity; cyber threats; risk management; cyber resilience; information systems resilience; financial sector cybersecurity.

Introduction

Information systems (IS) form the backbone of modern organisations. Information systems enable critical data management, business process support and communication across global networks (Luma & Abazi 2019). While IS aim to improve organisational operations, they also introduce the risk of exploitation, evidenced by over 20 000 cyberattacks in the past two decades and financial losses surpassing $12 billion (Natalucci, Qureshi & Suntheim 2024). Cyberattacks have emerged as one of the most formidable challenges to IS, given their frequency and sophistication (Jang-Jaccard & Nepal 2014). With their expansive digital footprints and valuable assets, financial institutions are desirable targets for cybercriminals seeking to exploit vulnerabilities for financial gain (Kelley 2022). Despite cybersecurity investments, financial institutions remain vulnerable to various cyber threats, including ransomware attacks, zero-day exploits and advanced persistent threats (APTs) (Laxman et al. 2023). The adaptability of cybercriminals often outperforms traditional cybersecurity measures (Laxman et al. 2023). Notable incidents such as the 2016 Bangladesh Bank heist, where hackers exploited the bank's SWIFT system to steal $101 million, and the 2017 Equifax data breach, which exposed sensitive financial data of millions, underscore the magnitude of these threats (Gaglione 2019; Maurer & Nelson 2021). The implications of cyberattacks mean that the protection of IS against exploitation and disruptions has become paramount (Sarkar et al. 2020).

Given the complex and evolving nature of cyber threats, relying solely on prevention is no longer sufficient. Instead, financial institutions must recognise the need to coexist with ongoing risks and adopt cyber resilience as a core strategy (Dupont 2019). A more comprehensive approach, such as resilience, is needed, as it is a mechanism to enable proactive strategies against cyber threats (Safitra, Lubis & Fakhrurroja 2023; Yulianto et al. 2025). A resilient approach focuses on immediate recovery and prevention, detection, adaptation and recovery from cyber threats (Ahmad, Hadgkiss & Ruighaver 2012). While considerable research has explored incident response and risk management, a notable gap remains in the development of holistic resilience frameworks that integrate these strategies into broader risk management systems (Dupont 2019; Langerman & Joseph 2025; Laxman et al. 2023; Sarkar et al. 2020). Given the financial sector's critical role in global economic stability (Dupont 2019; Gulyás & Kiss 2023; Natalucci et al. 2024), forward-looking resilience strategies that extend beyond the immediate response are urgently needed to ensure long-term operational preparedness. The increased focus on cybersecurity in the finance sector implies a shift towards proactive measures to mitigate potential threats and their impacts.

Research context and background

This section provides an initial background on how cyber threats have evolved in the financial sector and can be conceptualised within the resilience context for a robust cybersecurity environment.

The evolution of cyber threats

Cyber threats are becoming increasingly sophisticated and frequent. There has been a significant rise in monetary damage caused by cybercrime over the years, with losses reaching 12 500 million USD in 2023 (Petrosyan 2024a). This rise reflects a shift from traditional malware attacks to more complex, coordinated efforts such as APTs and ransomware, which often target critical infrastructure (Jang-Jaccard & Nepal 2014). To counter these evolving threats, Laxman et al. (2023) argued that adaptive and dynamic security measures are essential because static defences quickly become outdated. Advanced persistent threats are stealthy, persistent and often state-sponsored, posing severe risks to critical systems. Gan et al. (2023) noted that threats such as zero-day exploits and ransomware are increasingly complex, making them challenging to predict and counter effectively. Emerging technologies such as cloud computing, artificial intelligence (AI), Internet of Things (IoT) and big data have introduced new vulnerabilities, expanding the cyberattack surface (Aslan et al. 2023; Zhou et al. 2019). For instance, IoT's interconnectedness means that compromising one device can jeopardise an entire network. Sarkar et al. (2020) highlighted that while these innovations boost efficiency, they also complicate data protection. Financial institutions adopt these technologies; thus, they face unique cybersecurity challenges relative to protecting sensitive data and maintaining operational integrity. Financial institutions must develop adaptive, resilient strategies to keep pace with the evolving threats that address these complex risks.

Cyber threats in the financial sector

Literature discussing the vulnerability of the financial sector, including the works of Ali et al. (2019) and Maurer and Nelson (2020), highlights the sector's heightened exposure to cyber threats because of the high value of its assets and the critical nature of its operations. Between November 2021 and October 2022, this sector was the most globally targeted by basic web application attacks, with institutions experiencing 173 such incidents during this period (Petrosyan 2023). This underscores the sector's critical vulnerability and the need for enhanced cybersecurity to safeguard against prevalent threats. There has been a notable increase in ransomware attacks against financial institutions from 2021 to 2024. In 2024, approximately 65% of financial organisations globally reported experiencing ransomware attacks, marking a significant rise from 64% in 2023 and only 34% in 2021 (Petrosyan 2024b). This sharp rise reflects the increasing frequency and sophistication of attacks.

These insights underscore the escalating and complex nature of the cyber threats that the financial industry is facing. Natalucci et al. (2024) documented more than 20 000 cyberattacks in the past two decades, with financial losses surpassing $12 billion. These attacks range from high-profile heists, such as the $101 million stolen from the Bangladesh central bank, to disruptive ransomware campaigns. These data reveal the financial scale of cyber threats and the diverse tactics that cybercriminals employ. There is an urgent need for comprehensive resilience strategies that combine technological defences and organisational preparedness.

Maurer and Nelson (2021) highlighted that the sector's extensive digital footprint and global interconnectedness, while crucial for efficiency, also increase its vulnerability. As financial institutions adopt new technologies, the attack surface expands, making them more susceptible to sophisticated cyber threats (Ali et al. 2019).

Resilience strategies in the financial sector

The literature emphasises that resilience in IS encompasses more than technical defences; it requires a comprehensive approach that integrates organisational strategies and community involvement. Langerman and Joseph (2025) defined resilience as the ability of systems to anticipate, withstand, recover from and adapt to adverse conditions, highlighting that resilience involves proactive measures rather than merely responding after disruptions. Heeks and Ospina (2019) elaborate on resilience by focusing on developing countries and illustrating that resilience includes robustness, redundancy, resourcefulness and rapid response. Xu et al. (2024) provided an integrated framework for resilience research, demonstrating that resilience is a multidisciplinary field involving technical, social and organisational dimensions. Their citation network analysis revealed that effective resilience strategies require a holistic view that draws insights from diverse fields such as environmental science and social sciences.

Financial institutions can build systems capable of rapidly responding to emerging threats by adopting a holistic approach. This involves implementing cutting-edge technologies and fostering a culture of continuous improvement and preparedness across all levels of the organisation. The literature highlights several critical strategies to enhance financial institutions' resilience. These strategies focus on risk management frameworks, advanced technology, employee preparedness and industry collaboration. Various resilience strategies are employed to protect assets in the financial sector. These include adopting a combined risk management framework incorporating advanced technologies and incident response (Maurer & Nelson 2021). Advanced technologies such as AI, machine learning and blockchain can be utilised to enhance real-time threat detection, automate responses and secure transactions (Dupont 2019). Additionally, regular training and simulations can be implemented to minimise human error and foster a vigilant workforce ready to recognise and respond to threats (Gulyás & Kiss 2023). Furthermore, collaboration with other financial institutions and regulatory bodies is emphasised to share intelligence and best practices, ultimately strengthening collective resilience.

These components collectively create a multilayered defence system. Risk management frameworks guide the implementation of advanced technologies such as AI, which enhance real-time threat detection (Dupont 2019). Employee preparedness strengthens defences by equipping staff with the skills to respond swiftly to threats, whereas industry collaboration fosters adaptive, shared resilience against evolving threats. These elements enable financial institutions to anticipate, withstand, recover from and adapt to cyber threats, thus supporting ongoing stability and security.

Natale, Poppensieker and Thun (2022) emphasised the importance of integrating resilience strategies into organisational risk management for financial institutions to align resilience goals with overall business objectives and embed them across operations. The comprehensive framework, Dupont (2019) suggests, includes risk assessment, mitigation and continuous monitoring. Risk assessment identifies and evaluates cyber threats, and mitigation strategies, such as advanced security technologies, redundancy and incident response plans, help reduce their impact. Continuous monitoring supports early threat detection, enabling timely adjustments to resilience measures.

Coden et al. (2023) highlighted the importance of managing risks associated with third-party service providers, given financial institutions' growing reliance on external IT services. Regular audits, clear contractual cybersecurity expectations and contingency plans effectively address these dependencies. Additionally, Xu et al. (2024) advocated adaptive resilience strategies that use real-time monitoring and automated responses. Their approach calls for regular updates based on new threat intelligence and technological advancements to ensure that resilience measures respond dynamically to evolving threats.

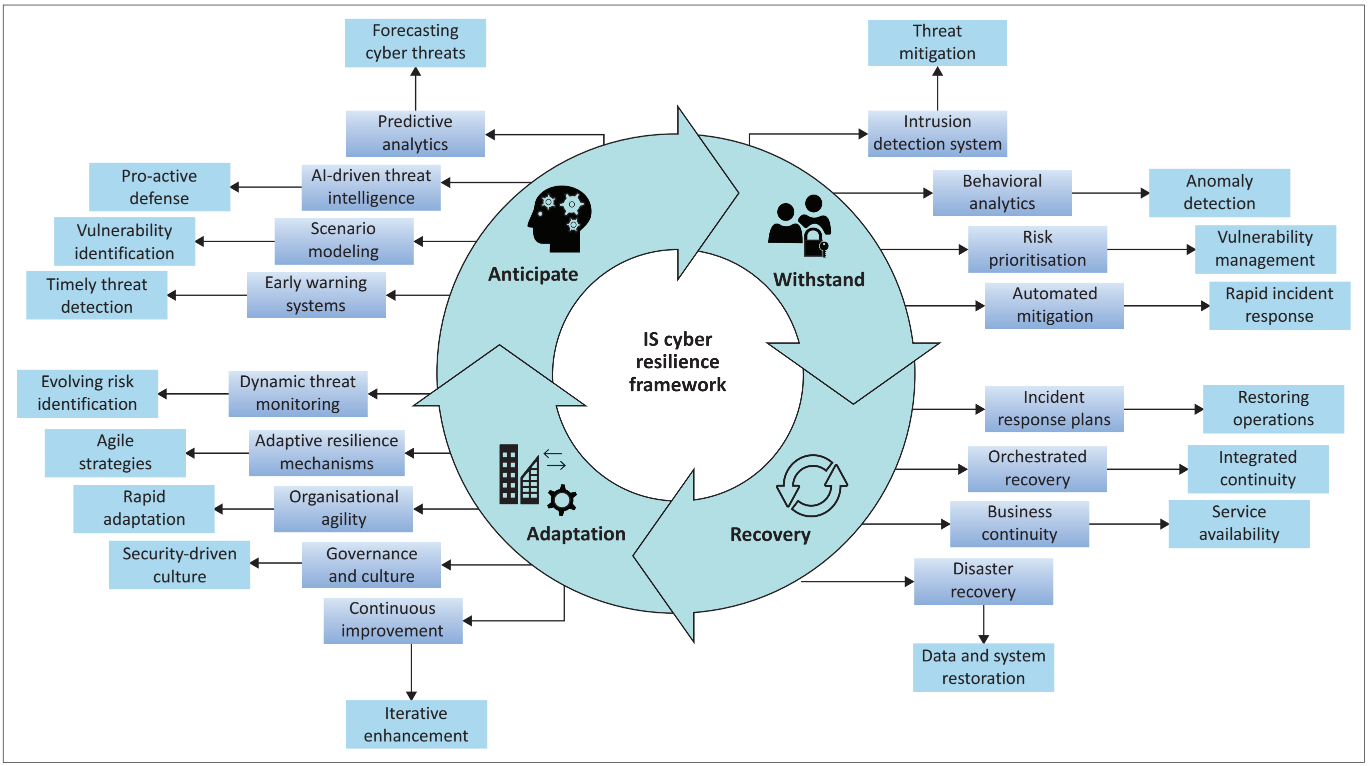
Effective governance is critical, Sarkar et al. (2020) emphasised. Leadership and organisational culture play pivotal roles, supporting a top-down approach that includes continuous training and awareness programmes to strengthen resilience across the workforce. The success of resilience integration can be assessed through metrics such as reduced downtime, reduced data loss and faster recovery. By embedding resilience within organisational risk management, financial institutions can enhance their capacity to withstand and recover from cyber incidents, ensuring operational stability and safeguarding critical assets.

Conceptualising information systems cyber resilience

Using a framework approach, this study conceptualises IS cyber resilience to enhance IS resilience by integrating adaptive and resilient strategies that surpass traditional cybersecurity measures. Figure 1 conceptualises IS cyber resilience to address the evolving nature of cyber threats, ensuring that financial institutions are better equipped to anticipate, withstand, recover from and adapt to such threats. By embedding these elements in a unified strategy, the proposed framework provides a holistic approach to safeguard critical IS infrastructure against increasingly sophisticated cyberattacks.

The key components of the framework are detailed as:

- *Anticipation:* Predictive models to predict potential cyber threats and their impacts. For instance, Danish (2024) highlighted the power of predictive analytics in real-time threat detection and response, which significantly improves the identification of advanced cyber threats. Zacharis, Katos and Patsakis (2024) emphasised the role of AI-driven threat intelligence in enhancing the accuracy and efficiency of predicting cyber incidents, enabling proactive defence measures.
- *Withstanding:* Implementing robust defence mechanisms to withstand cyberattacks. According to Zacharis et al. (2024), advanced machine learning techniques, such as Long Short-Term Memory (LSTM) networks, are effective in classifying intrusion detection patterns and forecasting cyber incidents. These methods help identify sophisticated threats and effectively mitigate their impacts.
- *Recovery:* Establish efficient recovery processes to restore operations after an attack. Dupont (2019) stressed the importance of developing robust incident response plans and backup systems to ensure continuity. The integration of advanced recovery techniques and regular drills can significantly reduce downtime and data loss during cyber incidents.



AI, artificial intelligence; IS, information system.

FIGURE 1: Conceptualising information systems cyber resilience.

- *Adaptation:* The resilience strategies must be continuously developed based on evolving threats and emerging technologies. Xu et al. (2024) emphasised the importance of adaptive resilience mechanisms that dynamically respond to new threats and update strategies based on the latest threat intelligence and technological advancements. Sarkar et al. (2020) highlighted the role of effective governance and organisational culture in implementing these adaptive strategies.

Financial institutions can significantly enhance their IS resilience by integrating these components into their broader organisational risk management frameworks. This comprehensive approach ensures that resilience measures align with overall business goals and are incorporated into all aspects of the organisation's operations.

The current fragmentation of cyber threat resilience literature implies that a better understanding is required (Ferdinand 2015). The financial sector, particularly, requires exploration in the cyber threat resilience context, given its critical role in global economic stability (Dupont 2019; Gulyás & Kiss 2023; Natalucci et al. 2024). Bibliometric analysis is an effective tool for systematically reviewing existing literature, identifying trends and pinpointing knowledge gaps within a specific research field (Donthu et al. 2021). This study employs bibliometric analysis to explore cyber threat resilience within the financial sector. The exploration enables the identification of influential works, emerging trends and gaps in the literature. Subsequently, this study addresses the following research questions (RQs), namely:

- **RQ1:** What is the volume, growth trajectory and geographic distribution of cyber threat resilience literature?
- **RQ2:** What journals, authors and articles have the greatest citation impact?
- **RQ3:** What is the intellectual structure of the cyber threats knowledge base?
- **RQ4:** What is the thematic evolution of cyber threat resilience?

Research methods and design

The methodology follows the guidelines of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 statement, which ensures transparency and rigour in the review process (Sohrabi et al. 2021). PRISMA provides a structured approach to identifying the state of knowledge on a given topic, thereby offering a comprehensive foundation for advancing the research landscape.

The documents for this bibliometric analysis were selected from the Scopus database, a highly regarded resource for peer-reviewed journals and conference papers in a wide array of academic fields (Pranckutė 2021). Scopus was selected because of its extensive coverage, indexing capabilities and continuous updates, making it ideal for literature reviews and bibliometric studies in the information systems and cybersecurity domain. Other databases, such as Web of Science, were considered, but Scopus offers broader coverage of the most relevant and impactful publications related to IS resilience in the financial sector (Mongeon & Paul-Hus 2016).

The search strategy was developed using a carefully constructed equation that combines relevant keywords and Boolean operators to ensure the retrieval of studies highly relevant to IS cyber resilience in the financial sector. The following search string was applied:

ALL (“Cyber Threats” OR “Cyber Attacks” OR “Cybersecurity” OR “Cyber Security” OR “Network Security” OR “IT Security” OR “Information Security” OR “Cyber Risk” OR “Technology Risk”)AND

(“Resilience” OR “Cyber Resilience” OR “Information Systems Resilience” OR “IT Resilience” OR “Systems Resilience” OR “Business Continuity” OR “Disaster Recovery” OR “Incident Response” OR “Risk Management” OR “Threat Intelligence” OR “Cyber Defence” OR “Resilience Strategies” OR “Mitigation Strategies” OR “Cybersecurity Frameworks”)AND

(“Financial Sector” OR “Banking Industry” OR “Financial Services” OR “Financial Institutions” OR “FinTech” OR “Banking Services” OR “Banking Sector” OR “Finance Industry” OR “Financial Technology” OR “Banking Institutions” OR “Investment Banking” OR “Central Banking”).

Articles focused on IS cybersecurity, cybersecurity and risk management in the financial sector are included. Non-peer-reviewed articles, reports, magazines, websites, opinion pieces and studies published before 2004 are excluded. Peer-reviewed journal articles and conference papers are also considered if they focus on IS resilience in the financial sector. The search was limited to English-language studies published between 2004 and 2024, capturing advancements in IS resilience strategies over the past two decades, focusing on cybersecurity developments and the evolving nature of threats and resilience frameworks in the financial sector.

The selection process was guided by the PRISMA flowchart (Figure 2) and proceeded through the following stages:

- *Identification:* A total of 288 records were retrieved from the Scopus database. Following an initial screening, 2 non-English documents and 58 documents that were not journal articles or conference papers were removed, leaving 228 documents for further analysis.
- *Screening and eligibility:* The 228 documents were reviewed based on their titles, abstracts and full texts. All documents met the inclusion criteria, and no further exclusions were necessary.
- *Inclusion:* All 228 documents were included in the final bibliometric analysis.

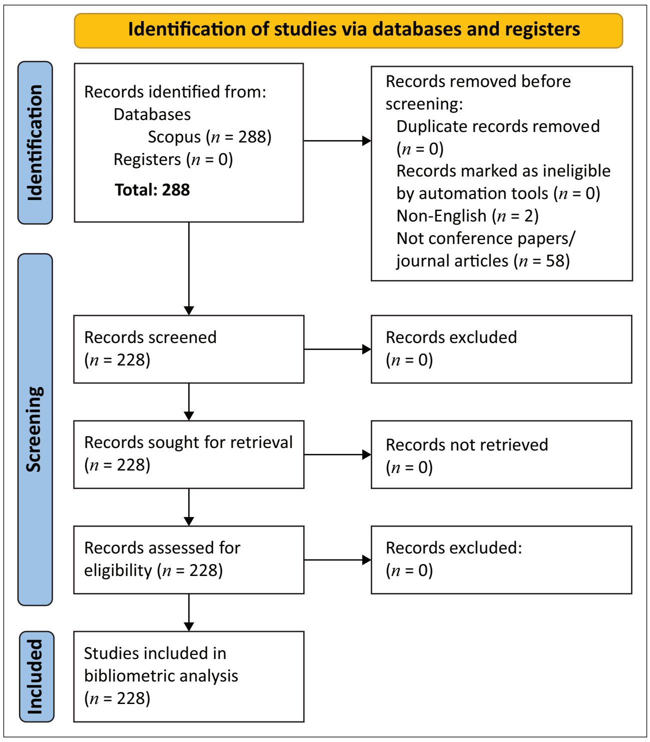
The selected documents were analysed using various bibliometric techniques to identify trends, patterns and relationships in the literature on IS cyber resilience in the financial sector. The analysis involved the following steps:

- Citation analysis identifies the most cited papers, authors and journals in the field, helping to highlight influential research (Jauhar et al. 2023).
- The coauthorship analysis examines collaboration patterns between authors, institutions and countries, providing insights into the social networks of researchers and revealing influential research groups (Kumar 2015).
- Co-word analysis analyses the co-occurrence of keywords within the selected papers, helping identify core thematic areas and emerging research topics related to IS cyber resilience and risk management (Wang et al. 2012).
- Network analysis maps the relationships between authors and institutions, visualising the connections and interactions within the field, and identifying central actors and collaborations (Jauhar et al. 2023).
- Co-citation analysis explores how frequently pairs of articles were cited together, providing a historical view of how research on IS resilience has evolved over time (Hou, Yang & Chen 2018).

The study employed Biblioshiny, a web-based interface for the Bibliometrix R package, which is widely used for bibliometric analyses (Aria & Cuccurullo 2017). Biblioshiny offers comprehensive features for performing citation analysis, co-word analysis and network visualisation, allowing for an in-depth exploration of the IS cyber resilience research landscape.

Ethical considerations

Ethical clearance to conduct this study was obtained from the University of Johannesburg College of Business and Economics


Identification of studies via databases and registers
Identification
Records identified from:
Databases
Scopus (n = 288)
Registers (n = 0)
Total: 288
Records removed before screening:
Duplicate records removed (n = 0)
Records marked as ineligible by automation tools (n = 0)
Non-English (n = 2)
Not conference papers/ journal articles (n = 58)
Screening
Records screened (n = 228)
Records excluded (n = 0)
Records sought for retrieval (n = 228)
Records not retrieved (n = 0)
Records assessed for eligibility (n = 228)
Records excluded: (n = 0)
Included
Studies included in bibliometric analysis (n = 228)

Source: Adapted from Sohrabi, C., Franchi, T., Mathew, G., Kerwan, A., Nicola, M., Griffin, M. et al., 2021, ‘PRISMA 2020 statement: What’s new and the importance of reporting guidelines’, *International Journal of Surgery* 88, 105918. https://doi.org/10.1016/j.ijsu.2021.105918

FIGURE 2: Preferred reporting items for systematic reviews and meta-analyses flowchart.

Research Ethics Committee (Ref. No. 2024AIS005). Regardless of the research endeavour, the ethical aspects of a study must be considered. This study only used bibliometric data (e.g. titles, abstracts, keywords and citations) acquired from Scopus, a publicly accessible academic database. No personal, confidential or sensitive data were collected or analysed, and the data were retrieved and used in accordance with the terms of service of the Scopus database. Author and institutional data were used to explore research networks, collaboration patterns and research productivity, and not to interrogate individual or institutional performance. Author names are displayed in accordance with accepted academic practice and are limited to descriptive and aggregate analyses. While this study did not involve human participants, experiments or interventions, ethical clearance was still sought to ensure ethical compliance.

Results

Segment one: The volume, growth trajectory and geographic distribution of cyber threat resilience literature

In this segment, the research analyses the volume, growth trajectory and geographic distribution of cyber threat resilience literature. The findings from the analysis indicate that the field is experiencing steady growth, with an annual growth rate of 19.95%, with a significant uptick after 2018. This indicates sustained scholarly interest in strengthening financial systems against cyber threats. The field has produced 228 documents from 186 unique sources, demonstrating several scholarly contributions. The average number of citations per document was 9.465 (indicating significant academic influence). A total of 635 authors contributed to the field, with an average of 2.94 coauthors per document, reflecting collaboration. International coauthorship is 17.98%, further emphasising the global effort to tackle shared cyber resilience challenges. In addition, the 766 unique keywords showcase the diversity of topics within the field, supported by 8386 references.

The United States (US) and India lead the way, with 339 and 222 citations, respectively, highlighting their significant contributions to the field. Additionally, significant citations from countries such as Australia (153) and Malaysia (129) further underscore the global nature of research in this field. However, the lack of substantial contributions from underrepresented regions, such as Africa and parts of South America, highlights a critical gap in global research efforts.

Segment two: Journals, authors and articles with the greatest citation impact

In this segment, the research analyses the journals, authors and articles with the greatest citation impact. Understanding the distribution of journals and conferences provides key insights into the evolution of cybersecurity research. The 'Journal of Risk Management in Financial Institutions' leads the way with five publications, followed by 'IEEE Access' and 'Information and Computer Security' with four each. On the other hand, the 'Association for Computing Machinery (ACM) International Conference Proceeding Series' reflects a shift to facilitating timely discussions on emerging issues, as conference contributions gained momentum after 2018. As cyberattacks become more sophisticated, the financial sector's need to address both security and resilience has become more urgent, driving the increase in research after 2018.

The results of the analysis of the most relevant authors provide insights into how contributions to the field are distributed, both in terms of individual and collaborative efforts. The fractionalised scoring system helps to break down the extent to which each author contributed to their respective publications. Authors, such as Berdyugin AA, who have a higher fractionalised score (0.83), indicate stronger individual contributions, highlighting their lead role in specific research outputs. In contrast, authors such as Bernard C, who had a lower fractionalised score (0.25), demonstrated more collaborative involvement, likely as part of larger research teams.

Table 1 highlights the 10 most globally cited documents in the dataset, reflecting the influential works shaping the field. The top three articles, Ahmad et al. (2012), Benaroch, Lichtenstein and Robinson (2006) and Al Nawayseh (2020) have 139, 139 and 114 citations, respectively. Interestingly, the top two articles were published before the uptick from 2018 and signify foundational studies that supported the increase in research around cyber threat resilience. The top two articles are also in highly cited and reputable

TABLE 1: Most globally cited documents.

Paper	DOI	Total citations	Total citations per year	Normalised total citations
Ahmad et al. 2012, Comput Secur	10.1016/j.cose.2012.04.001	139	10.69	2.64
Benaroch et al. 2006, Mis Quart Manage Inf Syst	10.2307/25148756	139	7.32	2.84
Al Naway Seh Mk, 2020, J Open Innov: Technol Mark Complex	10.3390/joitmc6040153	114	22.80	5.09
Noor et al. 2019, Future Gener Comput Syst	10.1016/j.future.2019.02.013	97	16.17	6.30
Abu MS, 2018, Indones J Electrical Eng Comput Sci	10.11591/ijeecs.v10.i1.pp371-379	95	13.57	7.92
Wang J, 2015, Mis Quart Manage Inf Syst	10.25300/MISQ/2015/39.1.05	93	9.30	4.27
Kandasamy et al. 2020, Eurasip J Inf Secur	10.1186/s13635-020-00111-0	92	18.40	4.11
Kanimozhi V, 2019, Proc Ieee Int Conf Commun Signal Process, ICCSP	10.1109/ICCSP.2019.8698029	91	15.17	5.91
Zhang Z, 2022, IEEE Access	10.1109/ACCESS.2022.3204051	79	26.33	8.32
Johnson ME, 2008, J Manage Inf Syst	10.2753/MIS0742-1222250205	49	2.88	2.72

Note: Please see the full reference list of this article Miya, N.F. & Joseph, N., 2025, 'Banking on resilience: 20 years of cybersecurity', *South African Journal of Information Management* 27(1), a2019. https://doi.org/ 10.4102/sajim.v27i1.2019 for more information.

journals, ‘Computers and Security’ and ‘Management Information Systems (MIS) Quarterly’. This further supports the foundational nature of the articles. Al Nawayseh (2020) has accumulated citations rapidly, although the article was published recently. The total citation per year (22.8) supports the article’s focus and reflects on the importance of cyber threat resilience in a financial context. Table 1 shows that six of the 10 articles were published after the initial lull from 2004 to 2017, as they range from 2018 to 2022.

Segment three: Intellectual structure of the cyber threats knowledge base

In this segment, the research analyses the intellectual structure of the cyber threats knowledge base. Co-citation analysis helps identify how foundational works are interrelated and form the foundation of scholarly discussions in the field. Alneyadi (2016) and ISO/IEC (2022) are the most frequently co-cited works, forming a singular cluster. The absence of other significant clusters shows fragmentation in the research, with key studies not being well integrated across the field.

The coauthorship network (Figure 3) reveals a fragmented research landscape in cyber resilience, showcasing many small, isolated clusters alongside a few larger interconnected groups. The small clusters indicate that researchers often work independently on specialised topics, leading to limited collaboration. In contrast, larger clusters represent groups that collaborate on comprehensive cybersecurity issues, enhancing knowledge-sharing. However, the overall prevalence of isolated clusters highlights the ongoing challenge of limited cross-group collaboration, hindering the potential for interdisciplinary integration in the field.

The coauthorship network by country highlights the US, India and the United Kingdom as leading hubs for international research collaboration. The connections between countries such as the US, Malaysia and China, as well as those between the United Kingdom and South Africa, suggest that cross-border collaboration is particularly vital in addressing shared cybersecurity challenges. However, countries such as Japan and Poland remain disconnected from major collaboration networks, indicating potential opportunities for more inclusive research efforts.

The co-word network in Figure 4 highlights the key terms and their connections in the field. The red cluster revolves around technical aspects of cybersecurity, with keywords such as ‘cyberattacks’, ‘AI’, ‘malware’, ‘intrusion detection’ and ‘blockchain’. This cluster highlights the emphasis on developing defensive strategies and technological solutions to address cyber threats. The presence of terms such as ‘machine learning’ and ‘decision-making’ underscores the growing reliance on advanced technologies to enhance cybersecurity systems’ ability to predict and mitigate potential attacks. This technical focus is crucial for financial institutions, which face constant cyber threats because of the sensitive nature of their data. Meanwhile, the blue cluster is centred on ‘risk management’ and ‘risk assessment’, highlighting a broader, more strategic approach to managing vulnerabilities in financial systems. This cluster also includes terms like ‘financial institutions’, ‘security of data’, and ‘incident response’, which are crucial in assessing and mitigating risks in financial systems. By focusing on risk assessment, this cluster demonstrates how financial sectors focus on proactive strategies to ensure system security against cyber threats.

The tree map in Figure 5 reinforces these insights, showing that ‘risk management’ and ‘cybersecurity’ are dominant themes, with ‘finance’ and ‘network security’ also playing crucial roles. The size of the boxes further illustrates the relative importance of these themes, indicating that ‘risk management’ (10%) and ‘cybersecurity’ (6%) are at the forefront of research discussions in this field.

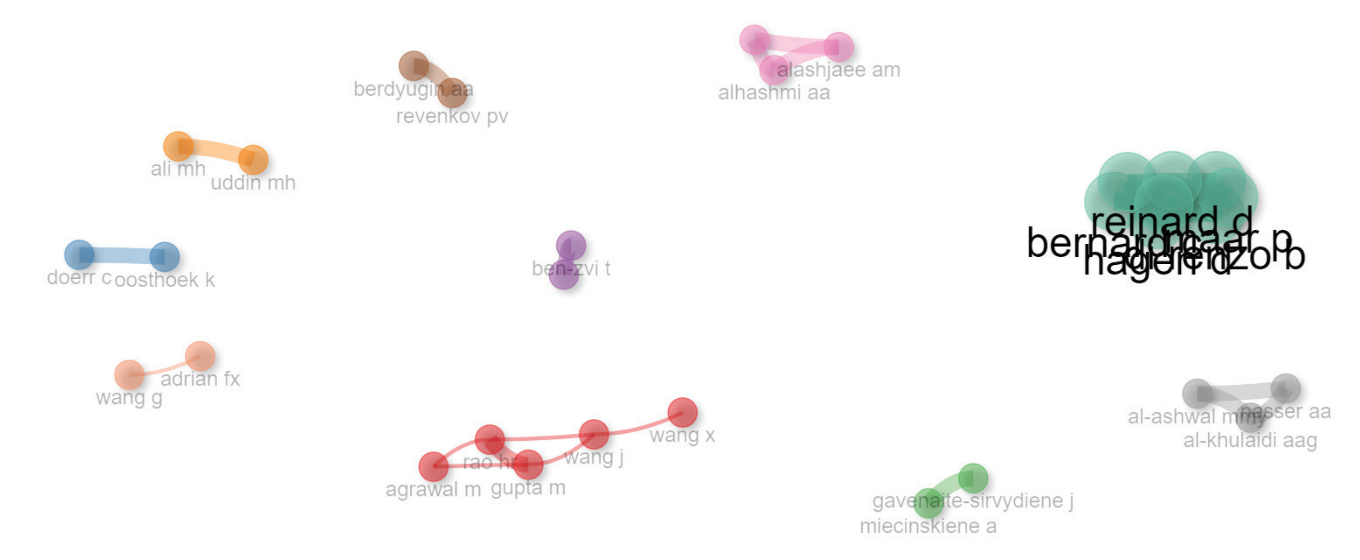


FIGURE 3: Coauthorship network.

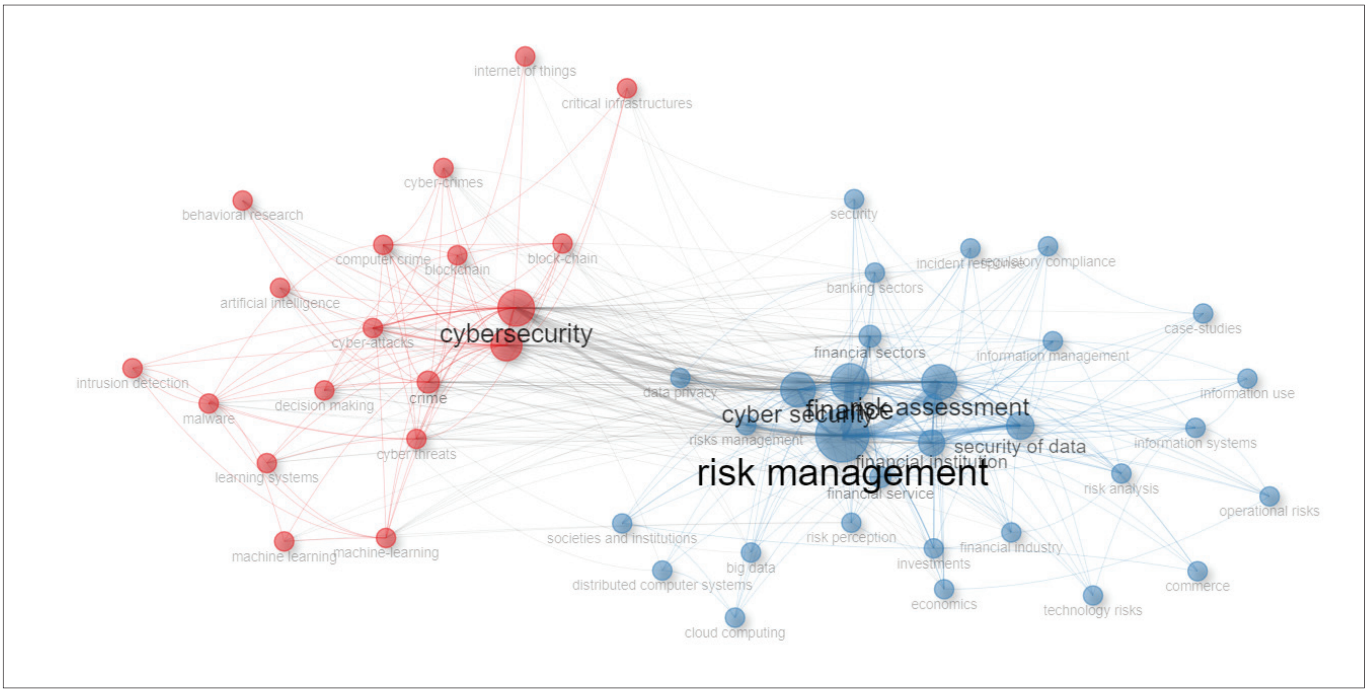


FIGURE 4: Co-word analysis network.

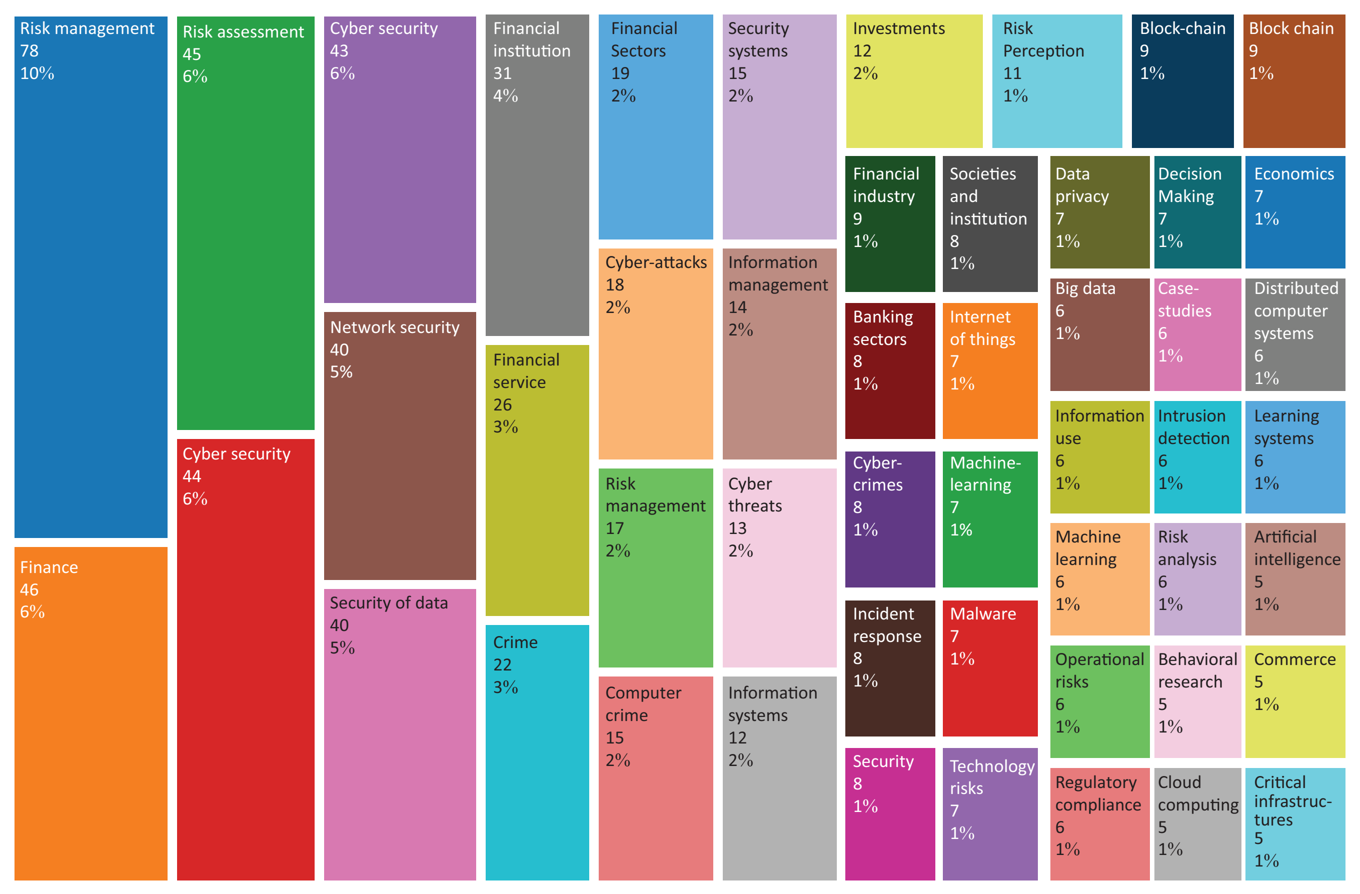


FIGURE 5: Tree map.

Segment four: Thematic evolution of cyber threat resilience

In this segment, the research analyses the thematic evolution of cyber threat resilience. The thematic evolution of research from 2004 to 2024 (Figure 6) highlights shifting priorities in cybersecurity. From 2004 to 2020, the emphasis was primarily on 'risk management' and 'critical infrastructures', with supporting themes such as 'security of data' and 'banking services' indicating early concern over financial institutions' vulnerability to cyberattacks. However, by 2021–2023, the focus shifted towards more technical themes, such as 'network security' and 'cybersecurity', reflecting the growing need for stronger defences in an increasingly digital landscape. This shift was a response to the rapid digitisation of financial services and the rise of online threats, particularly during the pandemic, when securing digital infrastructures became a top priority. As a result, earlier topics such as 'budget control' and 'human resource management' became less prominent as the focus was narrowed to addressing more pressing cybersecurity challenges.

Looking forward to 2024, new themes such as 'decentralised finance (DeFi)' and 'blockchain' are emerging. This evolution is driven by the emergence of new financial technologies that present unique security challenges. The shift towards blockchain and DeFi highlights how cybersecurity research is adapting to address the risks related to cryptocurrencies and distributed financial systems. While traditional themes such as 'risk management' remain relevant, they must now integrate these new technological risks to remain effective.

Figure 7 offers another layer of insight, showing how different topics are positioned on the basis of their relevance and development. Motor themes, such as 'cybersecurity', 'network security' and 'information systems' are highly developed and central to the field, driving much of the progress in securing digital infrastructures, particularly in the financial sector. Niche themes such as 'bitcoin', 'cyber criminals' and 'cybernetics' have less broad relevance but offer valuable insights into specific aspects of cyber threats. Basic themes, including 'risk management', 'finance' and 'risk assessment' are central yet underdeveloped, highlighting the need for more comprehensive research to enhance resilience frameworks in the financial industry. Overall, this thematic analysis highlights the need to integrate advanced technological solutions, such as machine learning and intrusion detection, with more traditional risk management frameworks to create a more resilient and secure financial sector.

Discussion

Research question 1: The volume, growth trajectory and geographic distribution of cyber threat resilience literature

The bibliometric analysis shows that cyber threat resilience research in the finance sector has experienced a steady growth rate of 19.95%, with a significant uptick after 2018. The annual

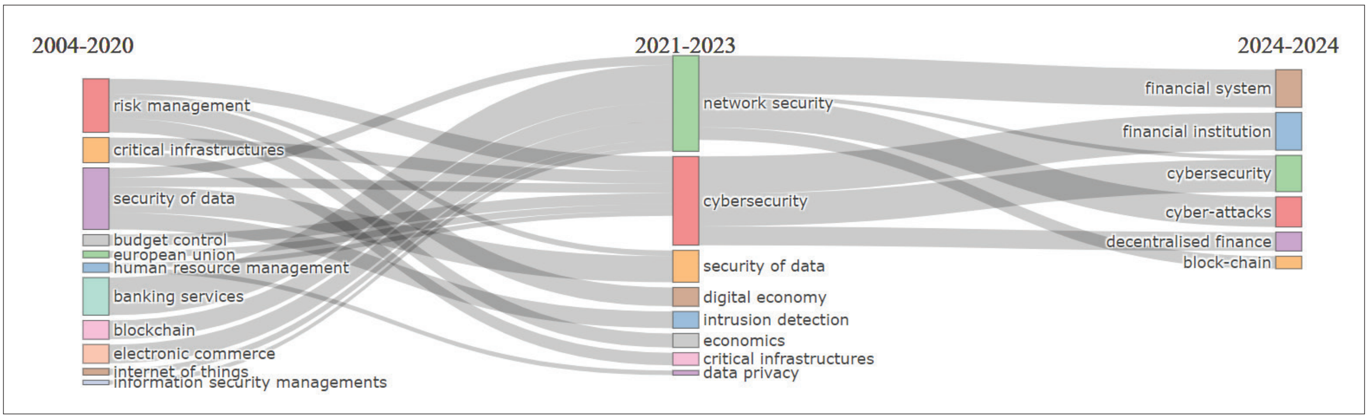


FIGURE 6: Thematic evolution from 2004 to 2024.

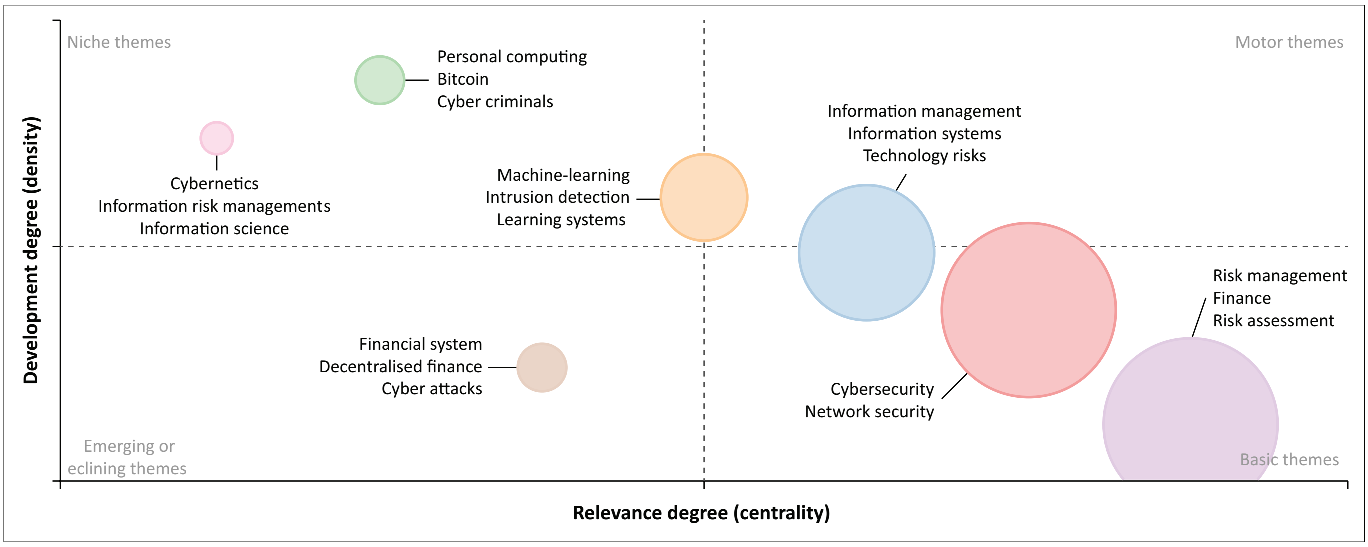


FIGURE 7: Thematic map of research themes.

scientific production uptick from 2018 corresponds to Savadatti, Srinivasan and Hu (2025), who reveal an uptick in 2017, but deviates from Savadatti et al. (2025), who reveal cybersecurity research steadily increased from 2013. This could be attributed to the focus of this study being on the finance sector, while Savadatti et al. (2025) were sector agnostic. However, this study and Savadatti et al. (2025) reveal a noticeable surge in publications, peaking sharply in 2023.

The increase in academic influence stems from 635 author contributions, with an average of 2.94 coauthors and 9.465 citations per document. Collaboration in cyber threat resilience is enabled by the geographic distribution of literature. The US and India have 339 and 222 citations, respectively, confirming the findings of Savadatti et al. (2025), revealing China, the US and India as significant contributors to cyber threat resilience research. The US, home to many of the world's largest financial institutions and tech companies, faces persistent cybersecurity threats, prompting extensive research into managing such risks. Similarly, India, with its rapidly growing tech industry and widespread adoption of digital services, has become a major target for cyber threats. This has driven Indian researchers and institutions to focus on enhancing cybersecurity measures to protect their digitising economy.

However, the lack of substantial contributions from underrepresented regions, such as Africa and South America, highlights a critical gap in global research efforts (Mushtaq & Shah 2025). The International Telecommunication Union (2024) acknowledges this as most African and South American nations are tier three (establishing) and four (evolving) regarding their Global Cybersecurity Index. The US and India, conversely, are tier one (role-modelling) nations, which is evident in their research stature in the field. Underrepresented regions are often affected by brain drain, where skilled researchers migrate to countries with better-funded research environments, such as the US and Europe, limiting the capacity of local institutions to produce cybersecurity research (Chand 2019). Although brain drain plays a significant role, other factors, such as limited access to research infrastructure and international collaboration opportunities, also contribute to the lower research output from these regions (Safitra et al. 2024; Savadatti et al. 2025). Addressing these challenges requires fostering international partnerships and increasing support for local research initiatives (Mushtaq & Shah 2025; Safitra et al. 2024). This gap presents opportunities for region-specific research and collaboration to address the unique cybersecurity challenges faced by these underserved areas.

Although the average document age is 4.09 years, the sustained scholarly output confirms the field's ongoing relevance as researchers continue to adapt to the fast-paced evolution of cyber threats. The growing recognition of cybersecurity as a critical issue, particularly within the financial sector, where cybersecurity threats are increasingly complex and frequent (Ali et al. 2019, Natalucci et al. 2024, Nobanee et al. 2023). The 2023 peak reflects the urgency to address cyber threat challenges, with researchers focusing on different approaches, such as resilience, to counteract the exploitation of IS. The increase in publications aligns with the global need for more robust and resilient cyber-resilient frameworks (Dupont 2019), demonstrating the critical role of research in developing strategies to safeguard financial institutions against evolving cyber risks.

Research question 2: Journals, authors and articles with the greatest citation impact

The 'Journal of Risk Management in Financial Institutions', 'IEEE Access', 'Information and Computer Security' and 'ACM International Conference Proceeding Series' are the most prevalent outlets for cyber threat resilience literature. 'IEEE Access' and 'Information and Computer Security' are consistent outlets for cyber threat resilience, as evident by Nobanee et al. (2023) and Savadatti et al. (2025). This study reveals that the 'ACM International Conference Proceeding Series' also plays a significant role, particularly in facilitating timely discussions on emerging issues. The emergence of the 'Journal of Risk Management in Financial Institutions' reflects the focus shift and importance of exploring cyber threat resilience in the financial sector. This highlights the delayed focus on cybersecurity in the financial sector, reflecting the growing urgency to address escalating cybersecurity risks in recent years. As cyberattacks become more sophisticated, the financial sector's need to address both security and resilience has become more urgent, driving the increase in research after 2018.

Regarding author impact, the results demonstrate a balance between individual leadership and collaborative efforts in advancing the field. This reflects the ongoing complexity of addressing cyber resilience, where teamwork across disciplines is crucial, but individual contributions are also pivotal in pushing forward specific innovations (Sepúlveda Estay et al. 2020). While collaboration is evident, there is a potential gap in fostering more cross-group collaboration (Salem et al. 2024). Many of the most cited researchers work within their institutional or regional bubbles, limiting the scope of interdisciplinary or cross-sector collaboration. Increasing collaboration between top individual contributors can lead to more comprehensive and innovative solutions to the complex cybersecurity challenges faced by financial institutions (Mohamed 2025).

Table 1 highlights the 10 most globally cited articles in the field. Ahmad et al.'s (2012) paper in 'Computer Security', with 139 citations, focuses on the challenges faced by incident response teams in supporting the organisational security function. This is crucial for building resilience by ensuring that organisations can effectively respond to and recover from cyber threats. Similarly, Benaroch et al.'s (2006) work on real options in IT risk management holds significant weight, with 139 citations, offering valuable insights into managing IT-related risks, which are essential for creating resilient infrastructures capable of withstanding evolving threats. Al Nawayseh's (2020) study on the factors influencing FinTech adoption during the COVID-19 pandemic has garnered 114 citations, reflecting its timely relevance in the intersection of financial technology and cybersecurity. The high total citation count and strong normalised citation scores, particularly for Noor et al. (2019) and Kandasamy et al. (2020), suggest that research related to cyber resilience frameworks and IoT risk assessments is gaining considerable traction. These studies collectively highlight the importance of interdisciplinary approaches, from AI-enhanced cybersecurity frameworks to signal processing techniques for preventing network intrusions, emphasising the need for robust resilience measures.

Research question 3: Intellectual structure of the cyber threats knowledge base

A key facet supporting the intellectual structure of the cyber threats knowledge base is the co-citation bibliometric indicator. The absence of other significant co-cited clusters, such as Alneyadi (2016) and Alneyadi (2022), reveals a lack of integration and collaboration. This may be because of the specialised nature of cyber resilience research, where different subfields, such as AI-driven security and blockchain resilience, evolve independently (Salem et al. 2024; Sepúlveda Estay et al. 2020; Taherdoost 2023). This limits cross-referencing between key works and leads to isolated areas of study.

Another contributing factor could be the lack of cross-disciplinary engagement. While cyber resilience overlaps with fields such as economics and risk management, the co-citation network indicates limited interaction between these disciplines (Salem et al. 2024). This may prevent the development of a comprehensive interdisciplinary framework that integrates both technical and strategic aspects of cyber resilience (Asmar & Tuqan 2024; Cremer et al. 2022; Li & Liu 2021; Shi & Wang 2025). Additionally, regional differences in research focus, such as the emphasis on local challenges in the US or Asia, may reduce global engagement and hinder the formation of broader co-citation patterns (International Telecommunication Union 2024).

To address these gaps, future research should focus on synthesising knowledge across different subfields and regions. Promoting cross-regional and cross-disciplinary collaborations would help to create a more connected and comprehensive framework, enhancing the global approach to addressing cyber resilience challenges (Mushtaq & Shah 2025; Safitra et al. 2024).

The fragmentation revealed in the coauthorship network (Figure 3) indicates that many researchers work in isolation, often focusing on specialised topics with limited collaboration across different teams. As highlighted in the co-cited clusters, this reflects the specialised nature of cyber resilience research, where key studies and researchers tend to remain disconnected, further emphasising the gap in collaboration across the field. Alternatively, the larger clusters represent research groups that have established broader collaborations, likely addressing more comprehensive issues related to cybersecurity, such as cybersecurity frameworks and systemic risks (Dupont 2019). Their interconnectedness facilitates knowledge-sharing and helps build a stronger foundation for core research. However, the prevalence of small, isolated clusters indicates that cross-group collaboration remains limited, preventing the field from achieving the benefits of interdisciplinary integration (Li & Liu 2021; Shi & Wang 2025). This fragmentation highlights the need for more cross-regional and cross-disciplinary collaboration, as mentioned in the analysis of the most cited countries, where regional differences in research focus were noted. Addressing these gaps could promote a more unified research landscape, integrate diverse expertise, and produce more globally relevant solutions for cyber resilience challenges in the financial sector.

The global map of coauthorship connections highlights the dominant roles of the US, India and the United Kingdom in cybersecurity research (Nobanee et al. 2023, Savadatti et al. 2025). The US is particularly noted for its extensive collaborations with countries such as Pakistan and Australia, while the UK maintains strong ties with the United Arab Emirates. These partnerships underscore the global reach of cybersecurity research, linking advanced economies with regions experiencing rapid digital transformation. However, there is a noticeable gap in collaborations with regions such as Africa and South America. This underrepresentation shows that while cybersecurity research is expanding globally, more inclusive efforts are required to address the unique challenges in these regions (Mushtaq & Shah 2025; Safitra et al. 2024). This is a common pattern where global collaboration requires urgent attention to ensure that underrepresented regions benefit from multiple perspectives around cyber threat resilience. This presents an opportunity for increased international cooperation, fostering a more comprehensive and diverse approach to tackling cybersecurity challenges (Li & Liu 2021; Shi & Wang 2025).

Figure 4 and Figure 5 contextualise two core patterns within the data, 'risk management' and 'cybersecurity'. Risk management and cybersecurity are intrinsically linked, as vulnerability assessment and risk management are crucial components of cybersecurity (Dupont 2019). Risk management embeds foundational concepts and practices that enable organisations to reflect on the intricate trifecta of people, process and technology. Despite this surge in academic interest, many highly cited works, such as Benaroch et al. (2006) and Ahmad et al. (2012), remain focused on incident response and risk management, leaving significant gaps in frameworks that integrate both prevention and recovery strategies (Dupont 2019). These insights reveal that cybersecurity research in the financial sector is multifaceted, blending technical defence mechanisms with strategic risk management frameworks (Asmar & Tuqan 2024; Shi & Wang 2025). However, the absence of terms such as 'cyber resilience' or 'resilience' in these visualisations suggests that while cybersecurity and risk management are well-researched, discussions about resilience are less prominent (Ferdinand 2015). This points to a gap in the literature and suggests that future research could focus more on resilience strategies to ensure that financial institutions are not only protected from cyber threats but also able to recover swiftly and maintain continuity when breaches occur (Dupont 2019). This highlights the need for future research to adopt a more proactive approach to cybersecurity, addressing the gaps in linking resilience strategies with broader risk management practices (Mohamed 2023).

The frequent appearance of terms such as 'incident response' and 'disaster recovery' indicates that these terms are the most widely employed resilience strategies. While Benaroch et al. (2006) and Ahmad et al. (2012) underscore the importance of having well-defined incident response plans, they also reveal a gap in integrated resilience frameworks that combine prevention, detection, adaptation and recovery. This gap underscores the need for further development of holistic strategies that are not only reactive but also proactive. Few studies link resilience strategies with broader risk management frameworks, indicating that although resilience has been increasingly discussed, it has not yet become a central component of risk management in financial institutions (Dupont 2019).

Research question 4: Thematic evolution of cyber threat resilience

Research trends show a shift from traditional cybersecurity topics to emerging areas such as decentralised finance (DeFi) and blockchain technology, which introduce new vulnerabilities (Zhou et al. 2019). The co-word analysis highlights the prevalence of threats such as 'malware', 'ransomware' and 'phishing', which severely impact system uptime and data integrity, often causing prolonged service disruptions. However, much of the current research remains reactive, concentrating on defensive measures or post-attack damage control rather than adopting a comprehensive resilience approach that includes detection, adaptation, and prevention. The results align with previous bibliometric analyses in cybersecurity, such as those by Ahmad et al. (2012) and Kandasamy et al. (2020), which highlighted the growing focus on technical defences such as intrusion detection and real-time monitoring systems. These are essential components of any cybersecurity strategy, particularly in the financial sector. This study adds new value by focusing on resilience in the financial context, which has been underexplored in previous research (Dupont 2019; Gulyás & Kiss 2023).

The existing literature has largely focused on cybersecurity measures and technical defences without giving sufficient attention to how organisations recover and maintain operations after a cyberattack (Asmar & Tuqan 2024; Ferdinand 2015; Laxman et al. 2023; Safitra et al. 2024; Sepúlveda Estay et al. 2020). The findings support a growing need for resilience frameworks that go beyond just technical defences and integrate broader organisational preparedness. This reflects the emerging consensus in cybersecurity research that resilience, ensuring continuity and post-incident recovery, is becoming as critical as preventative measures (Dupont 2019).

A key discrepancy between this study and earlier bibliometric studies is the underdeveloped focus on resilience in the broader cybersecurity landscape (Nobanee et al. 2023; Savadatti et al. 2025; Sulich, Zema & Kulhanek 2023). Although previous studies have mostly treated cybersecurity and risk management as distinct fields, this study highlights the need to merge resilience strategies with risk management. For instance, while technical solutions such as machine learning and blockchain continue to dominate current discussions, the resilience aspect remains fragmented, as shown by the co-citation analysis. This lack of integration calls for a more holistic approach to IS resilience, and future research should aim to better link these fields (Laxman et al. 2023).

Table 2 summarises the key insights and gaps identified, clearly indicating where this study's findings align with the body of knowledge and highlighting areas for further research.

Implications for academic research and industry practices

Based on the findings obtained regarding IS cyber resilience, the study provides significant implications in Figure 8 for academic research and industry practices. The study establishes through the TIPS™ framework (tt100 2025) that there is a need to consider technology, innovation, people and systems in managing cyber resilience.

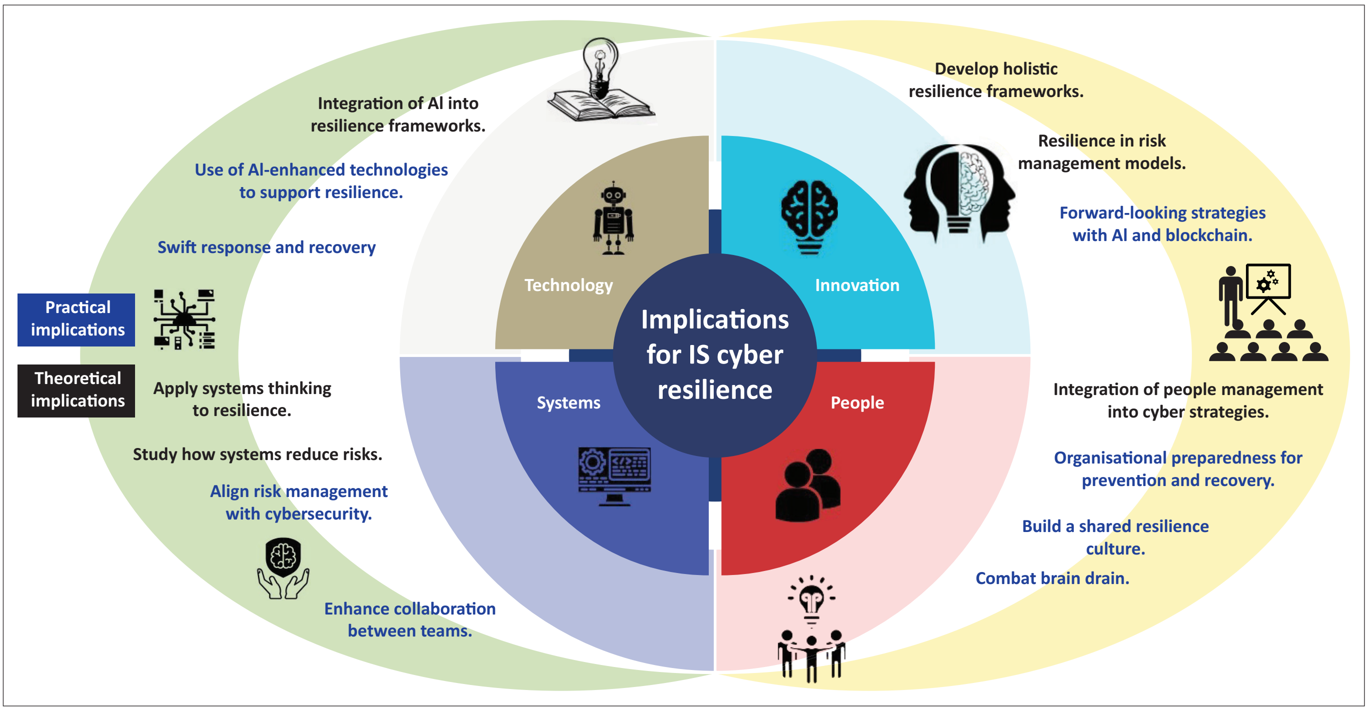
Technology

From a theoretical perspective, the fragmented nature of existing research highlights the need for cohesive frameworks that fully integrate advanced technologies (Cremer et al. 2022;

TABLE 2: Key insights and gaps identified in existing literature.

Key insights	Gaps identified
Prevalence of malware, ransomware and phishing as major cyber threats	Literature addresses these threats largely from a defensive or reactive perspective, focusing on incident response rather than proactive measures
Incident response and disaster recovery are the most common resilience strategies	Existing research lacks emphasis on integrated frameworks that combine prevention, detection, adaptation and recovery
Emerging technologies such as blockchain introduce new vulnerabilities	Research is fragmented, with little focus on how these technologies impact resilience frameworks in the financial sector
Artificial intelligence and machine learning are underutilised in resilience strategies	Practical adoption of AI-driven, real-time threat detection and response systems remains limited. Frameworks rarely incorporate advanced tools
Resilience is underdeveloped in terms of integration into broader organisational risk management	Existing studies treat resilience and risk management as distinct, failing to connect them in a cohesive framework
Lack of interdisciplinary collaboration and emphasis on human factors	Insufficient focus on workforce training, cross-disciplinary collaboration and integrating human factors in resilience frameworks
Systems thinking is rarely applied in resilience research	Current literature lacks emphasis on bridging organisational silos through systems thinking to create unified resilience strategies
Organisational preparedness for prevention and recovery is underdeveloped	Limited focus on fostering shared resilience cultures and addressing talent shortages, particularly in underrepresented regions

AI, artificial intelligence.


Implications for IS cyber resilience
Technology
Innovation
Systems
People
Practical implications
Theoretical implications
Integration of AI into resilience frameworks.
Use of AI-enhanced technologies to support resilience.
Swift response and recovery
Apply systems thinking to resilience.
Study how systems reduce risks.
Align risk management with cybersecurity.
Enhance collaboration between teams.
Develop holistic resilience frameworks.
Resilience in risk management models.
Forward-looking strategies with AI and blockchain.
Integration of people management into cyber strategies.
Organisational preparedness for prevention and recovery.
Build a shared resilience culture.
Combat brain drain.

AI, artificial intelligence; IS, information systems.

FIGURE 8: Implications for information systems cyber resilience.

Li & Liu 2021). Despite advancements in AI-driven cybersecurity, the underutilisation of AI and machine learning in resilience strategies, particularly for detecting and managing vulnerabilities, remains a research gap (Mohamed 2023). This presents an opportunity to develop more comprehensive models that enhance the understanding of cyber resilience and inform the development of more effective frameworks (Kaur, Gabrijelčič & Klobučar 2023). In practice, this fragmentation underscores the need for organisations to adopt AI-enhanced systems capable of real-time threat detection and response. The coauthorship analysis revealed that limited collaboration across research groups has slowed the practical adoption of these technologies. Increasing partnerships and cross-institutional collaboration can accelerate the development of real-time resilience frameworks (Sepúlveda Estay et al. 2020). In addition, ongoing training and education are essential to ensure that cybersecurity professionals and users effectively leverage these technologies (Jawhar et al. 2024).

Innovation

The shift towards innovations such as blockchain and machine learning, as highlighted in the thematic evolution, presents a critical opportunity for researchers (Taherdoost 2023). These technologies are not yet fully integrated into existing resilience frameworks, leaving a gap for scholars to develop holistic models that address the growing complexity of cyber threats, including zero-day vulnerabilities (Touré et al. 2024). Practically, while AI-driven innovations hold significant potential, their full impact is hindered by a lack of interdisciplinary collaboration, as noted in the coauthorship analysis (Salem et al. 2024). Financial institutions should adopt forward-thinking strategies that incorporate these innovations into their resilience frameworks (Asmar & Tuqan 2024; Shi & Wang 2025). For example, machine learning can be leveraged for predictive threat detection, and blockchain technology can enhance the security of financial transactions to help financial institutions stay ahead of emerging risks.

People

The coauthorship analysis highlights a shortage of collaboration across disciplines, indicating a theoretical need for better integration of people management into cyber resilience strategies (Dalal et al. 2022). Ensuring adequate human resources, both in terms of skills and organisational culture, are adequately addressed is essential for building effective resilience frameworks (Suwansrikham et al. 2020). Practically, the study shows that organisational preparedness for cyber resilience must extend beyond technology. A shared resilience culture, one that engages all employees in cybersecurity efforts, is crucial for preventing and responding to cyber threats (Cheng 2023). The brain drain and shortage of skilled cybersecurity professionals, particularly in underrepresented regions such as Africa and South America, underscore the need for greater investment in talent development and retention strategies (Furnell 2021). Addressing these human capital challenges will ensure that organisations have the expertise required to manage emerging threats effectively.

Systems

The systems aspect, as revealed by the co-citation and coauthorship analyses, exposes a fragmented approach to how different systems, such as risk management and cybersecurity, function together within organisations

(Kure, Islam & Razzaque 2018). Applying systems thinking can bridge these silos, ensuring that people, technology and processes are interdependent components of a unified cybersecurity strategy (Soomro, Shah & Ahmed 2016). A more cohesive approach is required to simplify the complexity introduced by modern cybersecurity challenges, including zero-day vulnerabilities (Atoum, Otoom & Abu Ali 2014). In practice, aligning risk management and cybersecurity systems is essential for organisations to respond more effectively to cyber threats. The findings support that enhanced collaboration between teams can lead to more comprehensive strategies addressing technical and organisational risks (Furnell 2021). By developing resilient systems that integrate these components, organisations can reduce operational silos and create a stronger, more adaptable defence against both current and future threats.

Ensuring rapid recovery after an attack is critical. Financial institutions must be prepared to recover quickly and minimise operational disruptions. Moving from fragmented, reactive approaches to proactive, strategic frameworks allows organisations to manage modern cyber threats more effectively. This unified approach ensures long-term resilience and enhances the overall security posture of financial institutions and other institutions.

Limitations and recommendations for future research

This study advances the understanding of cyber resilience in financial institutions, though it has several limitations. A primary limitation was the fragmented nature of resilience strategies in the literature, with limited focus on preventative measures such as detection and adaptation. This limitation restricted the study's ability to fully explore proactive threat mitigation. Future research should prioritise addressing the full resilience cycle to enable institutions to adopt more comprehensive, proactive approaches.

Another significant limitation was the disconnect between resilience strategies and broader organisational risk management frameworks. Resilience is often treated as a standalone element that is insufficiently connected to overall risk practices, which reduces its effectiveness. This lack of integration hindered the study's ability to fully address resilience within broader risk practices, as the current literature has yet to mature in linking these areas. Future studies should focus on developing cohesive frameworks that embed resilience within risk management and foster a unified approach to threat mitigation.

Methodologically, the study's reliance on Scopus may have excluded valuable non-English research, particularly from regions such as China and Russia, which have substantial cybersecurity expertise. Future research should incorporate multiple databases and include non-English publications to ensure a more inclusive, global perspective on resilience. Furthermore, although quantitative methods effectively identified key trends, they did not capture qualitative insights into how organisational culture and behaviour influence resilience. Future studies should adopt mixed methods that integrate qualitative insights from industry professionals to deepen understanding of resilience practices in real-world settings.

As cyber resilience continues to evolve, addressing these limitations will become crucial. By focusing on comprehensive preventative strategies, integrating resilience with organisational risk management and adopting a global, interdisciplinary approach, future studies can strengthen financial institutions' resilience frameworks. This unified approach is essential for institutions to prepare for and respond effectively to the complex cyber challenges that lie ahead.

Conclusion

The fragmented state of cyber threat resilience literature requires a better understanding of the field (Ferdinand 2015), especially within the financial sector context (Dupont 2019; Gulyás & Kiss 2023; Natalucci et al. 2024). This study aimed to explore cyber threat resilience within the financial sector, allowing for the identification of influential works, emerging trends and gaps in the literature. The growth trajectory of cyber threat resilience has grown exponentially since 2018, as digital transformation is a driving agenda for many financial organisations. Financial organisations have shifted from primarily financial service delivery to technology-oriented entities that enable financial services through technology. The cyber threat resilience focus is evident in tier one and role-model nations such as the US, India and China, but is lacking in most African and South American nations. Author collaboration and foundational articles are a testament to this, as research in the field is dominated and isolated to tier one nations. This does not bode well for the global financial sector and economy, where there are intricate geopolitical implications when financial IS are exploited and disrupted.

The bibliometric analysis contributes to the cyber threat resilience debate and reveals theoretical and practical gaps and insights. Theoretically, the study shows fundamental gaps in cybersecurity literature, including the absence of integrated frameworks combining prevention, detection, adaptation and recovery. The integration gap indicates a lack of systems thinking approaches to bridge organisational silos and fails to connect resilience with broader risk management theories. Overall, opportunities for comprehensive theoretical development are neglected, as research remains fragmented across disciplines. Practically, the analysis indicates that reactive approaches to cyber threats are predominant rather than proactive strategies. Artificial intelligence and machine learning remain underutilised in real-world resilience implementations, and organisational preparedness is lacking. Socio-technical challenges are evident, particularly talent shortages in underrepresented regions. There is insufficient focus on enabling and empowering shared resilience cultures and encouraging cross-disciplinary collaboration, both of which are essential for effective cyber threat resilience.

Acknowledgements

This article is based on research originally conducted as part of Ntokozo F. Miya's Honours research report entitled 'IS Cyber Resilience: A Financial Sector Exploration', submitted to the Department of Applied Information Systems, University of Johannesburg in 2024. The research study was supervised by Nazeer Joseph. The research has since been adapted for journal publication and serves as an articulation and extension of the research report.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

N.F.M. contributed to the conceptualisation, methodology, formal analysis, and writing of the original draft. N.J. contributed to the conceptualisation, methodology, writing of the review and editing, and supervision. N.F.M. and N.J. both contributed to the article, discussed the results, and approved the final version for submission and publication.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The data that support the findings of this study are available on request from the corresponding author, N.J.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. They do not necessarily reflect the official policy or position of any affiliated institution, funder, agency, or that of the publisher. The authors are responsible for this article's results, findings, and content.

References

Abu, M.S., Selamat, S.R., Ariffin, A. & Yusof, R., 2018, 'Cyber threat intelligence–issue and challenges', *Indonesian Journal of Electrical Engineering and Computer Science* 10(1), 371–379. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Ahmad, A., Hadgkiss, J. & Ruighaver, A.B., 2012, 'Incident response teams – Challenges in supporting the organisational security function', *Computers & Security* 31(6), 643–652. https://doi.org/10.1016/j.cose.2012.04.001

Al Nawayseh, M.K., 2020, 'Fintech in COVID-19 and beyond: What factors are affecting customers' choice of fintech applications?', *Journal of Open Innovation: Technology, Market, and Complexity* 6(4), 153. https://doi.org/10.3390/joitmc6040153

Ali, M., Mijwil, B., Buruga, B.A. & Abotaleb, M.M., 2019, 'A comprehensive review on cybersecurity issues and their mitigation measures in fintech', *Iraqi Journal for Computer Science and Mathematics* 5(3), Article 004. https://doi.org/10.52866/ijcsm.2024.05.03.004

Alneyadi, S., Sithirasenan, E. & Muthukkumarasamy, V., 2016, 'Discovery of potential data leaks in email communications', in *2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–10, IEEE, Surfers Paradise, QLD, Australia.

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

Aslan, A., Ozkan-Okay, M., Yilmaz, A. & E, A., 2023, 'A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions', *Electronics* 12(6), 1–42. https://doi.org/10.3390/electronics12061333

Asmar, M. & Tuqan, A., 2024, 'Integrating machine learning for sustaining cybersecurity in digital banks', *Heliyon* 10(17), e37571. https://doi.org/10.1016/j.heliyon.2024.e37571

Atoum, I., Otoom, A. & Abu Ali, A., 2014, 'A holistic cyber security implementation framework', *Information Management & Computer Security* 22(3), 251–264. https://doi.org/10.1108/IMCS-02-2013-0014

Benaroch, M., Lichtenstein, Y. & Robinson, K., 2006, 'Real options in information technology risk management: An empirical validation of risk-option relationships', *MIS Quarterly* 30(4), 827–864. https://doi.org/10.2307/25148756

Chand, M., 2019, 'Brain drain, brain circulation, and the African diaspora in the United States', *Journal of African Business* 20(1), 6–19. https://doi.org/10.1080/15228916.2018.1440461

Cheng, J., 2023, *Building cyberresilience from collaborative culture*, viewed 17 July 2025, from https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/building-cyberresilience-from-collaborative-culture.

Coden, M., Reeves, M., Pearlson, K., Madnick, S. & Berriman, C., 2023, *An action plan for cyber resilience*, viewed 17 July 2025, from https://sloanreview.mit.edu/article/an-action-plan-for-cyber-resilience/.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. et al., 2022, 'Cyber risk and cybersecurity: A systematic review of data availability', *The Geneva Papers on Risk and Insurance – Issues and Practice* 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dalal, R.S., Howard, D.J., Bennett, R.J., Posey, C., Zaccaro, S.J. & Brummel, B.J., 2022, 'Organizational science and cybersecurity: Abundant opportunities for research at the interface', *Journal of Business and Psychology* 37(1), 1–29. https://doi.org/10.1007/s10869-021-09732-9

Danish, M., 2024, *Enhancing cyber security through predictive analytics: Real-time threat detection and response*, viewed 17 July 2025, from arXiv.2407.10864.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N. & Lim, W.M., 2021, 'How to conduct a bibliometric analysis: An overview and guidelines', *Journal of Business Research* 133, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Dupont, B., 2019, 'The cyber-resilience of financial institutions: Significance and applicability', *Journal of Cybersecurity* 5(1), 1–17. https://doi.org/10.1093/cybsec/tyz013

Ferdinand, J., 2015, 'Building organisational cyber resilience: A strategic knowledge-based view of cyber security management', *Journal of Business Continuity & Emergency Planning* 9(2), 185–195.

Furnell, S., 2021, 'The cybersecurity workforce and skills', *Computers and Security* 100, 102080. https://doi.org/10.1016/j.cose.2020.102080

Gaglione, G.S., 2019, 'The Equifax data breach: An opportunity to improve consumer protection and cybersecurity efforts in America', *Buffalo Law Review* 67(4), 1133.

Gan, C., Lin, J., Huang, D.-W., Zhu, Q. & Tian, L., 2023, 'Advanced persistent threats and their defense methods in industrial internet of things: A survey', *Mathematics* 11(14), 3115. https://doi.org/10.3390/math11143115

Gulyás, O. & Kiss, G., 2023, 'Impact of cyber-attacks on the financial institutions', *Procedia Computer Science* 219, 84–90. https://doi.org/10.1016/j.procs.2023.01.267

Heeks, R. & Ospina, A.V., 2019, 'Conceptualising the link between information systems and resilience: A developing country field study', *Information Systems Journal* 29(1), 70–96. https://doi.org/10.1111/isj.12177

Hou, J., Yang, X. & Chen, C., 2018, 'Emerging trends and new developments in information science: A document co-citation analysis (2009–2016)', *Scientometrics* 115(2), 869–892. https://doi.org/10.1007/s11192-018-2695-9

International Telecommunication Union, 2024, *Global cybersecurity index 2024*, viewed 17 July 2025, from https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.

ISO/IEC, 2022, *Information security, cybersecurity and privacy protection — Information security controls. ISO/IEC 27002:2022*, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Geneva.

Jang-Jaccard, J. & Nepal, S., 2014, 'A survey of emerging threats in cybersecurity', *Journal of Computer and System Sciences* 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jauhar, S.K., Priyadarshini, S., Pratap, S. & Paul, S.K., 2023, 'A literature review on applications of industry 4.0 in project management', *Operations Management Research* 16(4), 1858–1885. https://doi.org/10.1007/s12063-023-00403-x

Jawhar, S., Miller, J. & Bitar, Z., 2024, 'AI-driven customized cyber security training and awareness', in *Proceedings of the 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, pp. 1–5, 7–9 February 2024.

Johnson, M.E., 2008, 'Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain', *Journal of Management Information Systems* 25(2), 97–124. https://doi.org/10.2753/MIS0742-1222250205

Kandasamy, K., Srinivas, S., Achuthan, K. & Rangan, V.P., 2020, 'IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process', *EURASIP Journal on Information Security* 2020(1), 1–19. https://doi.org/10.1186/s13635-020-00111-0

Kanimozhi, V. & Jacob, T.P., 2019, 'Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing', in *2019 International Conference on Communication and Signal Processing (ICCSP)*, pp. 0033–0036, IEEE, Chennai, India.

Kaur, R., Gabrijelčič, D. & Klobučar, T., 2023, 'Artificial intelligence for cybersecurity: Literature review and future research directions', *Information Fusion* 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kelley, P., 2022, *Evolution of cyber attacks and their economic impact*, Institute of Electrical and Electronics Engineers (IEEE), viewed 25 October 2024, from https://www.techrxiv.org/doi/full/10.36227/techrxiv.21670718.v1.

Kumar, S., 2015, 'Co-authorship networks: A review of the literature', *Aslib Journal of Information Management*, 67(1), 55–73. https://doi.org/10.1108/AJIM-09-2014-0116

Kure, H.I., Islam, S. & Razzaque, M.A., 2018, 'An integrated cyber security risk management approach for a cyber-physical system', *Applied Sciences* 8(6), 898. https://doi.org/10.3390/app8060898

Langerman, J. & Joseph, N., 2025, 'Operationalising information systems resilience within the financial services sector', in A. Nagar, D.S. Jat, D. Mishra, A. Joshi (eds.), *Intelligent Sustainable Systems. Worlds4 2024. Lecture Notes in Networks and Systems*, vol. 1179, Springer, Singapore.

Laxman, N., Krohmer, D., Damm, M., Schwarz, R. & Antonino, P.O., 2023, 'Understanding resilience: Looking at frameworks & standards – A systematic study from cyber perspective', in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, IEEE, Venice, Italy, pp. 295–300.

Li, Y. & Liu, Q., 2021, 'A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments', *Energy Reports* 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Luma, A. & Abazi, B., 2019, 'The importance of integration of information security management systems (ISMS) to the organization's enterprise information systems (EIS)', in *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, IEEE, Opatija, Croatia, pp. 1205–1208.

Maurer, T. & Nelson, A., 2020, *International strategy to better protect the financial system against cyber threats*, Carnegie Endowment for International Peace, Washington DC.

Maurer, T. & Nelson, A., 2021, *The global cyber threat to financial systems – IMF F&D*, viewed 17 July 2025, from https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.

Mohamed, N., 2023, 'Current trends in AI and ML for cybersecurity: A state-of-the-art survey', *Cogent Engineering* 10(1), 2272358. https://doi.org/10.1080/23311916.2023.2272358

Mohamed, N., 2025, 'Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms', *Knowledge and Information Systems* 67, 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

Mongeon, P. & Paul-Hus, A., 2016, 'The journal coverage of web of science and scopus: A comparative analysis', *Scientometrics* 106(1), 213–228. https://doi.org/10.1007/s11192-015-1765-5

Mushtaq, S. & Shah, M., 2025, 'Threats to the digital ecosystem: Can information security management frameworks, guided by criminological literature, effectively prevent cybercrime and protect public data?', *Computers* 14(2), 219.

Natale, A., Poppensieker, T. & Thun, M., 2022, *From risk management to strategic resilience*, McKinsey & Company, viewed 25 October 2024, from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/from-risk-management-to-strategic-resilience.

Natalucci, F., Qureshi, M.S. & Suntheim, F., 2024, *Rising cyber threats pose serious concerns for financial*, viewed 11 March 2025, from https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.

Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M. & Al Darmaki, A., 2023, 'Bibliometric analysis of cybercrime and cybersecurity risks literature', *Journal of Financial Crime* 30(6), 1736–1754. https://doi.org/10.1108/JFC-11-2022-0287

Noor, U., Anwar, Z., Amjad, T. & Choo, K.-K.R., 2019, 'A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise', *Future Generation Computer Systems* 96, 227–242. https://doi.org/10.1016/j.future.2019.02.013

Petrosyan, A., 2023, *Global industry sectors most targeted by basic web application attacks from November 2021 to October 2022*, viewed 17 July 2025, from https://www.statista.com/statistics/221293/cyber-crime-target-industries/.

Petrosyan, A., 2024a, *Annual amount of financial damage caused by reported cybercrime in U.S. 2001*, viewed 17 July 2025, from https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/.

Petrosyan, A., 2024b, *Rate of ransomware attacks in financial institutions worldwide 2021–2024*, viewed 17 July 2025, from https://www.statista.com/statistics/1460896/rate-ransomware-attacks-global/.

Pranckutė, R., 2021, 'Web of Science (WoS) and Scopus: The titans of bibliographic information in today's academic world', *Publications* 9(1), 12. https://doi.org/10.3390/publications9010012

Safitra, M.F., Lubis, M. & Fakhrurroja, H., 2023, 'Counterattacking cyber threats: A framework for the future of cybersecurity', *Sustainability* 15(18), 13369. https://doi.org/10.3390/su151813369

Safitra, M.F., Lubis, M., Fakhrurroja, H. & Yekti, Y.N.D., 2024, *Lessons from the past: A historical literature review on cyber resilience*, pp. 47–56, Springer Nature Singapore, Singapore.

Salem, A.H., Azzam, S.M., Emam, O.E. & Abohany, A.A., 2024, 'Advancing cybersecurity: A comprehensive review of AI-driven detection techniques', *Journal of Big Data* 11, 105. https://doi.org/10.1186/s40537-024-00957-y

Sarkar, A., Wingreen, S., Ascroft, J. & Sharma, R., 2020, 'Towards a practice-based view of information systems resilience using the lens of critical realism', *Proceedings of the 53rd Hawaii International Conference on Systems Sciences (HICSS-53)*, Grand Wailea in Maui, Hawaii, January 7–10, 2020.

Savadatti, S.G., Srinivasan, K. & Hu, Y.C., 2025, 'A bibliometric analysis of agent-based systems in cybersecurity and broader security domains: Trends and insights', *IEEE Access* 13, 90–119. https://doi.org/10.1109/ACCESS.2024.3520583

Sepúlveda Estay, D.A., Sahay, R., Barfod, M.B. & Jensen, C.D., 2020, 'A systematic review of cyber-resilience assessment frameworks', *Computers & Security* 97, 101996. https://doi.org/10.1016/j.cose.2020.101996

Shi, J. & Wang, Y., 2025, 'Academic exploration of blockchain and AI in financial services', *Journal of Electronic Business & Digital Economics*. https://doi.org/10.1108/JEBDE-08-2024-0023

Sohrabi, C., Franchi, T., Mathew, G., Kerwan, A., Nicola, M., Griffin, M. et al., 2021, 'PRISMA 2020 statement: What's new and the importance of reporting guidelines', *International Journal of Surgery* 88, 105918. https://doi.org/10.1016/j.ijsu.2021.105918

Soomro, Z.A., Shah, M.H. & Ahmed, J., 2016, 'Information security management needs more holistic approach: A literature review', *International Journal of Information Management* 36(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Sulich, A., Zema, T. & Kulhanek, L., 2023, 'Towards a secure future: A bibliometric analysis of the relations between cybersecurity and sustainable development', *Procedia Computer Science* 225, 1448–1457. https://doi.org/10.1016/j.procs.2023.10.133

Suwansrikham, P., Kun, S., Hayat, S. & Jackson, J., 2020, 'Dew computing and asymmetric security framework for big data file sharing', *Information* 11(6), 303.

Taherdoost, H., 2023, 'Blockchain and machine learning: A critical review on security', *Information* 14(5), 295. https://doi.org/10.3390/info14050295

Touré, A., Imine, Y., Semnont, A., Delot, T. & Gallais, A., 2024, 'A framework for detecting zero-day exploits in network flows', *Computer Networks* 248, 110476. https://doi.org/10.1016/j.comnet.2024.110476

Tt100, 2025, *Tips framework*, viewed 17 July 2025, from https://tt100.org/index.php/tips-framework/.

Wang, J., Gupta, M. & Raghav Rao, H., 2015, 'Insider threats in a financial institution: Analysis of attack-proneness of information systems applications', *MIS Quarterly* 39(1), 91–112. https://doi.org/10.25300/MISQ/2015/39.1.05

Wang, Z.-Y., Li, G., Li, C.-Y. & Li, A., 2012, 'Research on the semantic-based co-word analysis', *Scientometrics* 90, 855–875. https://doi.org/10.1007/s11192-011-0563-y

Xu, J., Ni, M., Zhu, D. & Yu, X., 2024, 'Overview of SQL injection attack detection techniques', in *Proceedings of the 2023 International Conference on Communication Network and Machine Learning (CNML '23)*, pp. 215–225, Association for Computing Machinery, New York, NY.

Yulianto, S., Soewito, B., Gaol, F.L. & Kurniawan, A., 2025, 'Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration: A paradigm shift in cybersecurity assessment', *Cyber Security and Applications* 3, 100077. https://doi.org/10.1016/j.csa.2024.100077

Zacharis, A., Katos, V. & Patsakis, C., 2024, 'Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle', *International Journal of Information Security* 23(4), 2691–2710. https://doi.org/10.1007/s10207-024-00860-w

Zhang, Z., Hamadi, H.A., Damiani, E., Yeun, C.Y. & Taher, F., 2022, 'Explainable artificial intelligence applications in cyber security: State-of-the-art in research', *IEEE Access* 10, 93104–93139. https://doi.org/10.1109/ACCESS.2022.3204051

Zhou, W., Jia, Y., Peng, A., Zhang, Y. & Liu, P., 2019, 'The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved', *IEEE Internet of Things Journal* 6(2), 1606–1616. https://doi.org/10.1109/JIOT.2018.2847733