Cent. Eur. J. Public Policy 2025; 19(2): 87-110
DOI: 10.2478/cejpp-2025-0010

Matúš Panko[1], Leoš Šafár[2], Michal Mešťan[3]*

Small Firms, Big Threats: Cybersecurity Research and the Role of Public Policy in the SME Sector

ABSTRACT: *Small-sized and medium-sized enterprises (SMEs) are vital to global economies but remain highly vulnerable to cyber threats due to limited resources, technical capacity, and awareness. This bibliometric study analyzes 245 peer-reviewed documents on SME cybersecurity published between 2005 and 2025, mapping the field through keyword co-occurrence, author productivity, citation patterns, and collaboration networks. Results show steady growth, with research output increasing at 16.7% annually. Core themes include awareness, governance, risk management, digital adoption, and Industry 4.0 integration, with a clear shift from technical toward strategic and human-centered approaches. Lotka's Law indicates fragmentation, as most authors contribute only once, underscoring the need for academic continuity. The United States, the United Kingdom, and South Africa dominate in volume, while France and Australia stand out for international collaboration. Influential contributors such as Spruit M and De Arroyabe JCF emphasize regulatory compliance and resilience. The literature highlights persistent challenges for SMEs in adopting standards like ISO 27001 and emerging technologies such as machine learning. Promising interventions include gamified training tools like CySecEscape 2.0 to strengthen awareness. This study advances understanding of SME cybersecurity research and calls for tailored, interdisciplinary strategies to enhance resilience, offering insights for policy, scholarship, and practice. The bibliometric evidence also reveals a growing recognition of the role of public policy and regulation in shaping SME cybersecurity practices. Highly cited works such as Kabanda et al. (2018), Heidt et al. (2019), Kljucnikov et al. (2019), and Tamvada et al. (2022) emphasize that national and European regulatory frameworks, including the NIS2 Directive and the Cyber Resilience Act, significantly influence SMEs' readiness, compliance behavior, and investment in security. These findings underline that effective cybersecurity strategies for SMEs require not only technological and organizational measures but also coherent public policy support and accessible institutional mechanisms.*

KEYWORDS: cybersecurity; SMEs; digital transformation; cybersecurity awareness; bibliometric analysis, public policy

RECEIVED 16 October 2025; **ACCEPTED** 22 November 2025.

INTRODUCTION

SMEs are integral to the global economy and represent more than 90% of businesses worldwide. Despite their economic significance, SMEs often face substantial challenges in implementing robust cybersecurity measures because of limited resources, expertise, and awareness (Gupta et al., 2018; Ponemon Institute, 2023). This vulnerability is exacerbated by the increasing sophistication of cyber threats, which exploit both technological weaknesses and human factors within organizations. The human element is a critical aspect of cybersecurity in SMEs. The development of a strong cybersecurity culture within organizations is essential for mitigating the risks associated with human behavior. Uchendu et al. (2021) emphasized the importance of cultivating a cybersecurity culture that encompasses employee awareness, management support, and continuous education to address security challenges effectively. Regulatory frameworks also play a pivotal role in shaping cybersecurity practices among SMEs. The European Union's Network and

1 Technical University of Košice, Faculty of Economics, Department of Banking and Investment, Němcovej 32, 040 01 Košice, Slovakia; Email: matus.panko@tuke.sk; ORCID: https://orcid.org/0000-0002-5976-0675

2 Technical University of Košice, Faculty of Economics, Department of Banking and Investment, Němcovej 32, 040 01 Košice, Slovakia; Email: leos.safar@tuke.sk; ORCID: https://orcid.org/0000-0001-8466-0644

3 Corresponding author*, Matej Bel University in Banská Bystrica, Faculty of Economics, Department of Finance and Accounting, Tajovského 10, 975 90 Banská Bystrica, Slovakia; Email: michal.mestan@umb.sk; ORCID: https://orcid.org/0000-0002-4974-2254

Information Security (NIS) Directive, along with the General Data Protection Regulation (GDPR), has established a comprehensive approach to cybersecurity governance. These regulations mandate that member states develop national cybersecurity strategies, including risk management and incident response mechanisms, thereby influencing SMEs to adopt more structured cybersecurity measures. Digitalization presents both opportunities and challenges for SMEs. While adopting digital technologies can increase operational efficiency and market reach, it also introduces new cybersecurity risks. Markopoulou et al. (2019) highlighted that SMEs pursuing digitalization and internationalization must navigate complex cybersecurity landscapes, necessitating tailored strategies to safeguard their digital assets. The implementation of Industry 4.0 technologies further complicates the cybersecurity landscape for SMEs, particularly in emerging economies. Tamvada et al. (2022) identified critical risks associated with adopting advanced technologies, such as the internet of things (IoT) and big data analytics, including inadequate infrastructure and a lack of skilled personnel, which can hinder effective cybersecurity implementation. Education and awareness programs are vital in enhancing cybersecurity resilience among SMEs. Bada and Nurse (2019) propose high-level cybersecurity education frameworks tailored for SMEs, emphasizing the need for continuous training and awareness to combat evolving cyber threats. Innovative approaches, such as gamified learning, have been explored to improve cybersecurity awareness. Löffler et al. (2021) introduced "CySecEscape 2.0," a virtual escape room designed to increase cybersecurity awareness among SMEs, demonstrating the potential of interactive learning methods in fostering a security-conscious culture. Given these multifaceted challenges, a bibliometric analysis focusing on keywords such as "cybersecurity in SMEs," "information security awareness," "insider threat," and "software supply chain attack" can provide valuable insights into the current research landscape. Bibliometric methods enable the mapping of knowledge domains, identification of influential publications, and detection of research trends over time. This analysis is essential for informing both academic inquiry and policy development, ensuring that cybersecurity strategies are effectively tailored to the unique needs and constraints of SMEs.

While existing studies predominantly address technical, organizational, and human factors of cybersecurity in SMEs, considerably less attention has been given to the influence of public policy frameworks on firms' cybersecurity practices and readiness. The regulatory environment—shaped by instruments such as the EU NIS Directive, the General Data Protection Regulation (GDPR), and most recently the NIS2 Directive—has become a central determinant of cybersecurity behavior across the European SME landscape. These policy instruments not only establish minimum standards of protection but also foster a culture of compliance, incentivize investment in digital security, and enable coordinated responses through national cybersecurity strategies (Markopoulou et al., 2019; Carrapico & Barrinha, 2017; ENISA, 2025).

However, the extent to which public policy initiatives translate into improved cybersecurity capacity at the SME level remains unclear. Many small firms lack the financial, technical, or administrative capacity to comply with complex regulations, resulting in uneven implementation across sectors and countries (Uchendu et al., 2021). Furthermore, the interaction between top-down regulation and bottom-up organizational practices is underexplored in academic literature. To address this research gap, the present study extends its analytical scope by considering how public policy and state-level interventions shape cybersecurity awareness, compliance, and resilience among SMEs. By incorporating this dimension, the study aims to bridge bibliometric evidence with the policy environment, enabling a more holistic understanding of the socio-technical and institutional forces influencing SME cybersecurity. This broader perspective contributes to identifying how regulatory frameworks can be optimized to support SMEs in achieving sustainable digital resilience within the evolving European cybersecurity landscape.

The remainder of this paper is structured as follows. Section 2 reviews the relevant literature and conceptual background on cybersecurity in SMEs. Section 3 describes the research design and the PRISMA methodology employed. Section 4 presents the bibliometric and content analysis results. Section 5 discusses the key findings in light of current challenges and policy developments. The final section concludes with implications for SMEs, policymakers, and future research.

LITERATURE REVIEW AND THEORETICAL BACKGROUND

SMEs represent a vital component of national and global economies, contributing significantly to employment, innovation, and GDP. However, their cybersecurity posture remains a critical vulnerability, as SMEs are often under-resourced and underprepared to manage increasingly sophisticated cyber threats (Uchendu et al., 2021). Research consistently shows that SMEs lack formalized security policies, dedicated IT staff, and adequate awareness of the threats they face, which places them at greater risk than larger enterprises (Bada & Nurse, 2019). A foundational element in addressing this vulnerability is the development of a robust cybersecurity

culture. According to Uchendu et al. (2021), cybersecurity culture refers to the shared values, attitudes, and behaviors that shape how individuals and organizations understand and respond to cybersecurity challenges. In SMEs, fostering such a culture requires strong leadership support, clear communication of responsibilities, and systematic employee engagement through training and feedback mechanisms. However, these conditions are rarely met, as cybersecurity is often perceived as a purely technical issue rather than an organizational imperative. Thus, cybersecurity education and awareness programs play pivotal roles in improving SMEs' resilience. Bada and Nurse (2019) emphasize the importance of designing training initiatives tailored to the specific needs and capabilities of SMEs, with an emphasis on practicality, simplicity, and behavioral outcomes. Their framework recommends short, interactive training sessions focused on common threats such as phishing, social engineering, and poor password practices. These interventions have been shown to significantly reduce human error incidents and foster more secure daily operations.

In addition to internal organizational strategies, the broader regulatory and policy environment plays a critical role in shaping cybersecurity practices among SMEs, particularly within the European Union. One of the most significant regulatory instruments in this regard is the Directive on Security of Network and Information Systems (commonly known as the NIS Directive), which came into force in 2016 as the EU's first piece of legislation specifically addressing cybersecurity. The NIS Directive establishes baseline obligations for operators of essential services and digital service providers, including requirements related to risk management, incident reporting, and cooperation with national authorities. While SMEs are not the primary targets of the directive, they are nonetheless impacted indirectly, especially those operating in supply chains connected to critical sectors or providing digital services. As Carrapico and Barrinha (2017) argue, the directive's broader goal is to foster a culture of cybersecurity compliance and preparedness throughout the European digital ecosystem, including its peripheral actors such as SMEs. The implementation of the directive, however, has revealed significant asymmetries in compliance capacity. Many SMEs lack the administrative infrastructure, financial resources, or expertise to fully interpret and act upon the regulatory guidance provided by national cybersecurity agencies. Consequently, compliance has been uneven, with some SMEs embracing best practices, whereas others remain unaware of even minimal regulatory expectations (Carrapico & Barrinha, 2017).

To support smaller entities in navigating these regulatory demands, the European Union Agency for Cybersecurity (ENISA) has played an increasingly central role. ENISA has developed numerous tools, publications, and frameworks aimed at improving cyber hygiene across all organizational sizes. These include sector-specific guidelines, practical risk assessment methodologies, and awareness-raising campaigns tailored to nonexpert audiences. For example, ENISA's guides for SME cybersecurity provide step-by-step recommendations that account for limited budgets and human capital. Despite these efforts, the practical uptake of ENISA resources among SMEs remains limited. Studies suggest that many small firms are either unaware of ENISA offerings or find them too general or demanding to implement efficiently. There is also a disconnect between regulatory intentions and operational feasibility, as even simplified frameworks may require more time and knowledge than SMEs can realistically allocate (Uchendu et al., 2021). This illustrates a recurring tension in cybersecurity governance—between harmonized regulatory ambitions at the EU level and the diverse, often fragmented, operational realities of SMEs. Therefore, while the NIS Directive and ENISA represent important strides toward a more integrated and secure European digital infrastructure, their effectiveness in the SME sector remains contingent upon further localization, simplification, and support. Future policy refinements must consider SME-specific constraints and provide not only frameworks but also actionable implementation pathways adapted to firms with limited cybersecurity maturity.

Digitalization is another crucial dimension of cybersecurity in SMEs. As Westerlund (2020) illustrates, digital technologies enable SMEs to expand their market reach, particularly through online platforms and e-commerce. However, this expansion simultaneously increases exposure to cyber risks. SMEs frequently adopt digital tools without integrating appropriate cybersecurity measures, leading to vulnerabilities in areas such as data protection, supply chain management, and third-party integrations. The rapid pace of digital transformation often outstrips the development of cybersecurity capabilities, creating a gap between operational ambition and protective measures. This gap becomes even more pronounced in the context of Industry 4.0. The adoption of interconnected systems, smart devices, and data analytics offers numerous operational benefits, yet SMEs in emerging economies often encounter barriers to secure implementation. Tamvada et al. (2022) highlighted financial constraints, technological inertia, and limited cybersecurity awareness as key obstacles to the safe integration of Industry 4.0 technologies. Their findings underline the need for cybersecurity-by-design principles to be embedded into digital innovation strategies from the outset. To manage the complexity of modern cyber threats, the concept of cyber resilience has gained prominence in the academic and policy discourse. Carías et al. (2020) propose a systematic approach to operationalizing cyber resilience in SMEs, incorporating practices such as proactive risk assessment, incident response planning, and continuity of operations. Their model emphasizes integration with existing business processes and

scalability on the basis of firm size and sector. However, the adoption of resilience strategies is still limited often due to perceptions of high implementation costs and delayed return on investment.

Empirical studies provide insight into how SMEs implement cybersecurity standards in practice. Antunes et al. (2021), focusing on SMEs in Portugal, demonstrate that adoption of the ISO/IEC 27001 standard enhances both external trust and internal risk management. However, the uptake of such standards remains low, hindered by the misconception that international compliance frameworks are suitable only for larger organizations. Innovative approaches to cybersecurity training, such as gamified learning, offer promising alternatives for SMEs with limited training budgets. Löffler et al. (2021) introduced CySecEscape 2.0, a virtual escape room designed to improve cybersecurity awareness through interactive scenarios. Such tools increase user engagement and knowledge retention, particularly among nontechnical staff, and represent a scalable solution to the challenge of raising awareness in resource-constrained environments.

The adoption of advanced technologies, particularly those based on machine learning (ML), holds considerable promise for enhancing cybersecurity capabilities in SMEs. ML-based systems are capable of performing tasks such as anomaly detection, behavioral analysis, and predictive threat modeling with a high degree of accuracy and adaptability. These functionalities enable organizations to proactively identify and mitigate cyber threats in real time, reducing the likelihood and impact of breaches. However, integrating ML technologies into the cybersecurity strategies of SMEs remains challenging. A key barrier is the lack of specialized internal expertise to implement, monitor, and maintain these systems. Unlike large enterprises with dedicated security teams, SMEs often depend on generalist IT personnel or third-party providers, limiting their ability to manage complex tools. Additionally, the financial costs associated with acquiring and operating ML-driven platforms, such as computing infrastructure, data processing capabilities, and licensing, are frequently beyond the reach of smaller firms.

Infrastructure limitations further restrict the adoption of ML-based solutions. Many such applications demand significant computational power and storage that typical SME IT environments cannot support. As a result, even motivated SMEs may struggle to operationalize advanced technologies without external assistance. In light of these constraints, there is a growing need for simplified, cost-effective ML cybersecurity solutions tailored to the needs of SMEs. These should be user-friendly and scalable and require minimal technical oversight, enabling SMEs to benefit from ML-enhanced protection without deep technical involvement. Cloud-based services, pretrained models, and plug-and-play detection systems represent promising approaches to democratizing access to advanced cybersecurity tools. The cybersecurity environment in which SMEs operate is shaped by a complex and evolving interplay of technical, organizational, regulatory, and economic factors. Challenges in this domain are not limited to technology alone; rather, they are deeply intertwined with aspects of organizational culture, employee behavior, compliance requirements, and strategic decision-making. Addressing these challenges calls for an integrated response that combines innovation in cybersecurity tools with structural reforms and targeted capacity building, both at the firm level and within the broader policy landscape. As cyber threats continue to escalate in scope and complexity, SMEs require security solutions that are not only technologically robust but also adaptable to their specific operational contexts. Ensuring long-term cybersecurity and resilience in this sector will depend on coordinated action across academia, industry, and the government to promote secure, inclusive, and sustainable digital ecosystems. Based on the above discussion, we state the following research questions:

RQ1: What are the most prominent thematic clusters and keyword patterns characterizing cybersecurity research in the context of small and medium-sized enterprises (SMEs)?

RQ2: Who are the most influential authors, and how do citation-based indicators (e.g., h-index, g-index, m-index) reflect scholarly impact within the SME cybersecurity research domain?

RQ3: How is research on SME cybersecurity geographically distributed across countries, and what patterns of international collaboration can be observed?

RQ4: Which publications form the intellectual and conceptual foundation of SME cybersecurity research, and how their influence has evolved?

RQ5: How do public policy frameworks at the European and national levels influence the cybersecurity practices, compliance behavior, and resilience of small and medium-sized enterprises?

Cent. Eur. J. Public Policy 2025; 19(2): 87-110
DOI: 10.2478/cejpp-2025-0010

METHODOLOGY AND DATA

Approach and analytical tools

To explore the intellectual structure and research evolution of cybersecurity in the context of SMEs, this study employs bibliometric analysis as the primary methodological approach. As a systematic and quantitative method for evaluating scientific literature, bibliometrics complements traditional literature reviews by enabling the identification of research clusters, intellectual linkages, and collaborative networks within the academic community (Passas, 2024; Linnenluecke et al., 2019).

For the analysis, the Bibliometrix R-package was utilized within the RStudio environment. This open-source tool allows for comprehensive bibliometric and scientometric analysis, including co-authorship networks, keyword co-occurrences, source dynamics, and thematic evolution. By leveraging the analytical and visualization capabilities of Bibliometrix, the study was able to generate descriptive statistics, conceptual structure maps, and collaboration networks, offering deeper insights into the knowledge base, research trends, and intellectual connections in the field (Aria & Cuccurullo, 2017).

Dataset Scope and Filtering Strategy

The final dataset for this bibliometric study comprises 245 peer-reviewed journal articles published between 2005 and 2025, all of which are focused on the theme of cybersecurity as it relates to SMEs. Data were collected through targeted keyword searches from two thematic clusters that were carefully selected from terms designed to capture the technical, behavioral, and organizational dimensions of cybersecurity. These included terms such as cybersecurity in SMEs, phishing, insider threat, legacy system vulnerabilities, software supply chain attack, weak passwords, cyber literacy, and the human factor in cybersecurity. The initial keyword search generated a pool of 286 documents, which were systematically filtered on the basis of the following criteria (see Table 1).

Tab. 1: Filter settings on the Web of Science platform.

Search timeframe	**2005 to June 2025**
Document types	Journal articles, conference proceedings
Language	English
Fields	Topic (TS): titles, abstracts, author keywords, Keywords Plus
Thematic area	**Sample keywords**
Small and medium enterprise	TS=(("small business*" OR "small enterprise*" OR "medium business*" OR "medium enterprise*" OR SME OR SMEs OR "micro enterprise*" OR "micro business*" OR "micro, small and medium enterprise*" OR MSME OR MSMEs OR "small and medium-sized business*" OR "small and medium-sized enterprise*" OR "small-to-medium business*" OR "small-to-medium enterprise*" OR SMB OR SMBs)
	NEAR/10
Cybersecurity	("cybersecurity" OR "cyber security" OR "cyber-sec*" OR "cyber threat*" OR "cyber attack*" OR "cyber incident*" OR "digital secur*" OR "information secur*" OR infosec OR "network secur*" OR "IT secur*" OR "data secur*" OR "computer secur*")) AND TS=("threat*" OR "vulnerabilit*" OR "risk*" OR "resilien*" OR "awareness" OR "readiness" OR "preparedness" OR "incident response" OR "compliance" OR "standard*" OR "framework*" OR "solution*" OR "strategy" OR "strategies" OR "management" OR "governance" OR "best practice*" OR "implementation")

Source: Prepared by the authors.

Selection of keywords

A systematic approach was applied in selecting the set of keywords for the bibliometric analysis, with the aim of comprehensively covering the thematic scope of cybersecurity in the context of small and medium-sized enterprises (SMEs). The selected terms reflect not only the technical aspects of cybersecurity but also the organizational, behavioral, and human factors that are critical in this domain. The core set of keywords consisted of terms directly related to cybersecurity in SMEs, incorporating various combinations of expressions such as "SME," "small business," "micro enterprise*"* and "cybersecurity," "cyber threat," "digital security,"* connected via proximity operators (e.g., NEAR/10) to ensure coverage of terminological variations within the academic literature. A second group of keywords focused on the technical vulnerabilities and common cybersecurity threats faced by SMEs. This included terms such as threat, vulnerability, risk, resilience, framework, compliance, and incident response, which were selected for their high relevance to contemporary security discourse. The third group addressed the human factor and cybersecurity awareness of SMEs. Keywords such as awareness, training, readiness, governance, and best practices were included to capture the importance of organizational culture, education, and employee behavior in shaping the overall cybersecurity posture. The keyword selection was designed to enable a comprehensive mapping of the relevant literature and to facilitate the identification of research trends, key topics, and potential gaps in the field.

Interdisciplinary scope and PRISMA guidelines

The resulting dataset reflects the inherently interdisciplinary nature of cybersecurity within SMEs. Research in this area intersects with technological vulnerabilities, human behavior, organizational policy, and regulatory frameworks. The dataset spans disciplines such as IT management, cybersecurity governance, organizational psychology, information systems, education, and legal compliance, capturing the complexity of cybersecurity readiness in SMEs.

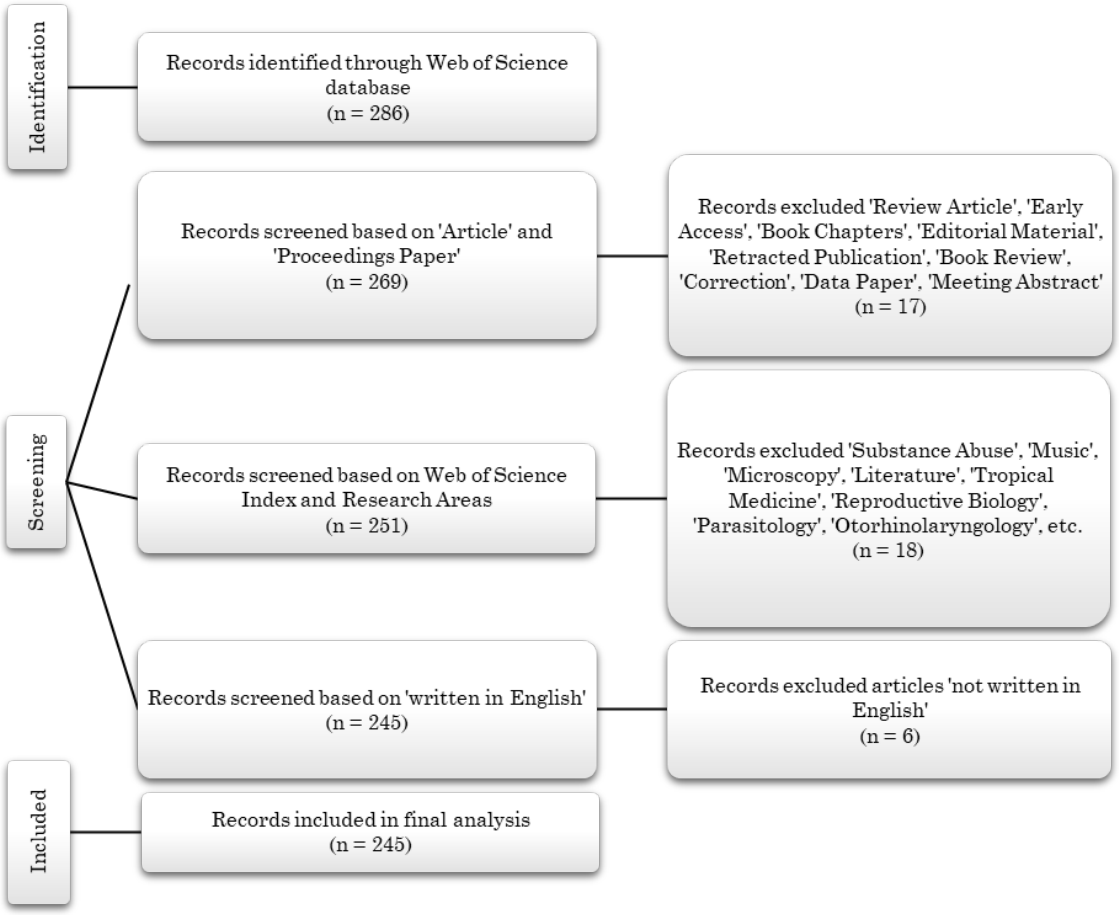
The selection process followed PRISMA guidelines to ensure transparency and replicability. In the identification stage, 286 records were retrieved from the Web of Science database. After the results were limited to journal articles and conference proceedings, 17 nonresearch outputs (e.g., review articles, editorials, book chapters) were excluded, leaving 269 records. During the screening stage, 18 documents unrelated to the subject area (e.g., articles on substance abuse, literature, or parasitology) were removed from the research areas. Finally, 6 articles not written in English were excluded, resulting in a final dataset of 245 records included in the analysis.

Temporal scope and thematic coverage

The temporal range of the dataset spans from 2005 to June 2025, enabling a longitudinal analysis of thematic evolution, including emergent and maturing topics such as phishing, vulnerabilities related to remote work, and the increasing focus on human-centered cybersecurity interventions (e.g., awareness, training, and security culture). The inclusion of both technical (e.g., IT security, web application vulnerability, legacy systems) and behavioral (e.g., information security awareness, human factor, governance) terms ensures a holistic perspective on the challenges SMEs face in securing their information infrastructure. This comprehensive filtering approach resulted in a dataset comprising 245 documents, involving 787 authors, and capturing 794 author keywords and 221 Keywords Plus. The methodologically rigorous, thematically coherent, and empirically grounded dataset serves as a solid foundation for analyzing scholarly output, research impact, and intellectual developments in the cybersecurity SME domain.

Table 2 provides an overview of the bibliometric characteristics of the final dataset comprising 245 documents published between 2005 and June 2025. These documents were sourced from 194 different publication outlets, including academic journals and conference proceedings. Annual scientific production has exhibited a robust growth trend, with an average annual growth rate of 16.71%. The average age of the documents is 5.47 years, indicating a relatively recent focus on the topic. On average, each document received 7.84 citations, and the dataset as a whole contained 8,219 references. In terms of content, the dataset includes 221 Keywords Plus (extracted from titles of cited references) and 794 author-supplied keywords, reflecting a diverse range of thematic interests within the cybersecurity-SME intersection. The authorship analysis reveals contributions from 787 unique authors, with only 14

Fig. 1: PRISMA flow diagram.



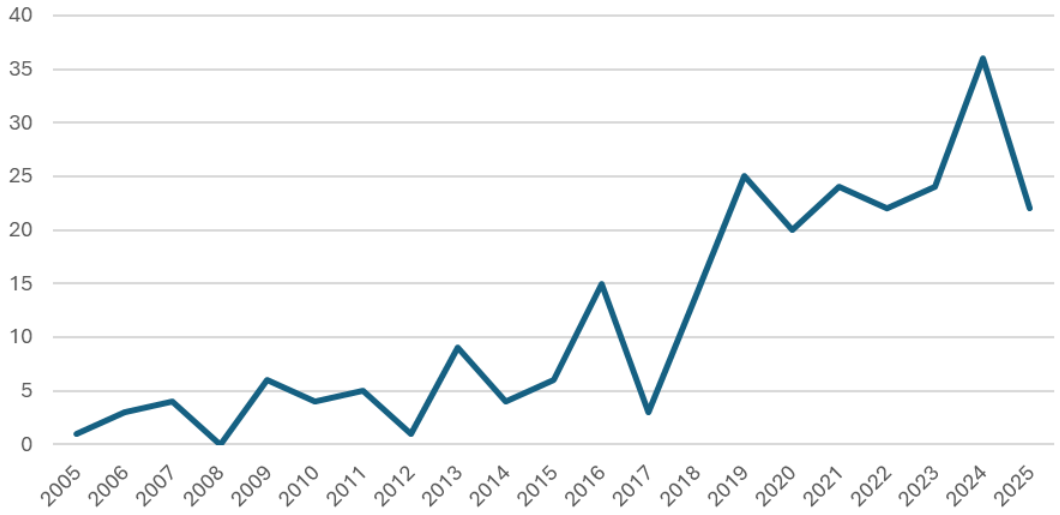
Source: Prepared by the authors.

Tab. 2: Bibliometric summary of the dataset.

Description	Results	Description	Results
Timespan	2005–2025	Authors	787
Sources (journals, books, etc.)	194	Authors of single-authored docs	14
Documents	245	Single-authored docs	16
Annual growth rate %	16.71	Co-authors per doc	3.63
Document average age	5.47	International co-authorships %	20.41
Average citations per doc	7.837	Article	112
References	8219	Article; proceedings paper	1
Keywords Plus (ID)	221	Proceedings paper	132
Author's keywords (DE)	794		

Source: Prepared by the authors.

Fig. 2: Publication trend.



Source: Prepared by the authors.

documents authored by a single researcher. Out of the 245 documents, 16 were single-authored, while the average number of co-authors per document was 3.63. Notably, 20.41% of the publications involved international co-authorship, indicating a significant degree of global collaboration. Regarding document types, the dataset consists of 112 journal articles, 132 conference proceedings, and 1 hybrid document labeled as both an article and a proceedings paper. This distribution underscores the relevance of both academic and applied research in this domain.

Figure 2 illustrates the annual evolution of academic publications focusing on cybersecurity in the context of SMEs from 2005 to 2025. The trend demonstrates a clear increase in research output over time, with notable fluctuations and several periods of accelerated growth. While the early years (2005–2014) are characterized by relatively low and inconsistent publication activity, a gradual upward trajectory becomes evident from 2015 onward. A sharp increase in publications is observed between 2018 and 2020, followed by another significant surge between 2022 and 2024, culminating in a peak in 2024, with more than 35 documents published. This peak reflects heightened scholarly interest in the intersection of digital transformation and cybersecurity challenges within SMEs—potentially influenced by external factors such as the COVID-19 pandemic, increased remote work, and global policy focus on digital resilience. Although a decline is visible in 2025, this may be partially attributed to data incompleteness for the current year. Overall, the trend reveals a growing academic recognition of the relevance of cybersecurity for SMEs, with a compound annual growth rate of approximately 16.7%. Despite this positive momentum, the historical underrepresentation of this topic—especially in the first half of the analyzed period—suggests that the field remains relatively underexplored. Continued research is necessary to address the evolving threat landscape and support SMEs in developing effective cyber resilience strategies through evidence-based insights and interdisciplinary frameworks.

RESULTS

Keyword analysis

The analyzed table captures the 20 most frequently occurring keywords identified through bibliometric analysis of documents related to cybersecurity and small and medium-sized enterprises (SMEs). These keywords, extracted and clustered via VOSviewer, offer a window into the prevailing research themes, terminological patterns, and conceptual priorities within the literature. The keywords "cybersecurity" (69 occurrences) and "information security" (48 occurrences) clearly dominate the landscape, reflecting the central

disciplinary anchor of the dataset. The co-occurrence of both terms underlines the close interlinkage between practical cybersecurity implementations and the broader domain of information protection. Interestingly, "cyber security" appears as a separate variant (13 occurrences), signaling inconsistencies in author keyword formatting, which is common in bibliometric datasets but conceptually convergent. Keywords directly referencing small and medium-sized enterprises—"SMEs" (47 occurrences) and "SME" (38 occurrences)—demonstrate the corpus's strong alignment with the SME context. Although variably abbreviated or singular/plural, these terms confirm the analytical focus on business entities that typically face resource constraints and heightened vulnerability to cyber threats. Their consistent appearance affirms the importance of understanding cybersecurity within the structural and strategic limitations unique to SMEs. Risk-related keywords such as "risk management" (15 occurrences) and "risk" (13 occurrences) highlight the literature's preoccupation with threat mitigation and organizational resilience. These themes reflect a mature stage in the research trajectory, where cybersecurity is increasingly framed not just as a technical problem but also as a managerial and operational challenge requiring proactive governance. The appearance of "awareness" (14) and "cybersecurity awareness" (9) points to the growing recognition of human-centered vulnerabilities in cybersecurity research. In the SME environment, where formal IT departments may be absent or limited, raising awareness among nontechnical staff becomes a vital line of defense against cyber threats such as phishing or insider attacks. Keywords such as "adoption" (11), "technology" (11), "innovation" (9), and "Industry 4.0" (10) signal a research emphasis on the integration of digital technologies within SMEs. This aligns with global trends in smart manufacturing and digital transformation, where the benefits of innovation are paralleled by heightened exposure to cyber risks. The link between cybersecurity and technology adoption is thus a recurring point of analysis. The presence of terms such as "management" (27), "impact" (14), "model" (10), and "business" (9) suggests that scholars increasingly conceptualize cybersecurity not only as a technical safeguard but also as a strategic, managerial concern. The modeling of cybersecurity risks and their business impacts is particularly relevant in helping SMEs allocate limited resources toward effective digital protection.

The keyword occurrence distribution confirms that current research on SMEs and cybersecurity spans both technical domains (e.g., information security, risk, technology) and organizational/strategic considerations (e.g., management, awareness, adoption). The integration of Industry 4.0 and digital adoption themes suggests a strong orientation toward innovation-driven transformation within SMEs. Moreover, repeated references to awareness and risk management emphasize the importance of holistic, organization-wide cybersecurity preparedness. Together, these findings point to a multidimensional research landscape—one that bridges technology, strategy, and human factors in addressing the cybersecurity needs of SMEs.

The co-occurrence network graphically maps the conceptual structure of the literature on cybersecurity in the context of SMEs on the basis of keyword frequency and linkage. The largest node, "cybersecurity," sits at the center of the network, reflecting its dominant role in the research field. Its strong connections to multiple clusters highlight its interdisciplinary nature and centrality in various thematic discussions. Adjacent to "cybersecurity" are keywords such as "risk management," "cybercrime," "machine learning," and "digitalization," indicating frequent co-occurrence and suggesting a close thematic relationship. This cluster emphasizes both the technical and strategic aspects of cybersecurity, particularly its intersection with digital transformation and intelligent systems.

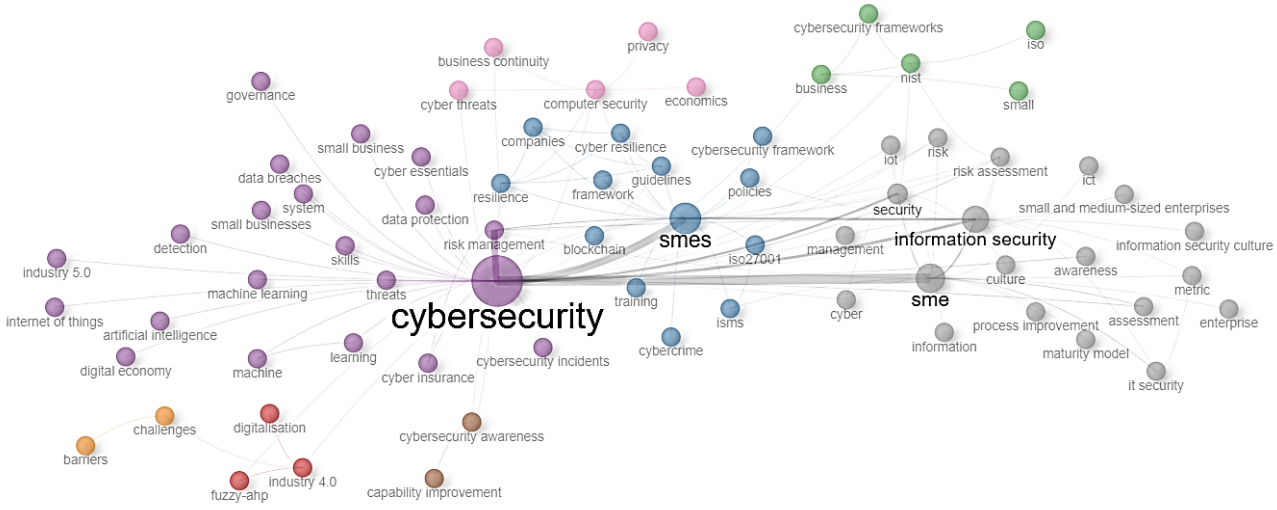
The keywords "SMEs," "SME," and "information security" form another dense cluster, reinforcing the core focus on SMEs. These terms are strongly linked to themes such as "ISO 27001," "training," "management," and "cybersecurity framework," highlighting organizational responses to cybersecurity challenges, including the implementation of standards and policy-driven practices. Smaller, more peripheral clusters—such as those around "governance," "industry 5.0," "internet of things," and "privacy"—indicate emerging or niche areas of interest. Although less central, they suggest directions for future exploration, particularly in terms of adapting to new technologies and societal demands. The color-coded groupings reveal thematic subdomains, including technical mechanisms (e.g., AI, blockchain), strategic implementation (e.g., policies, training), and socio-organizational concerns (e.g., awareness, culture, governance). This structure points to a growing integration of technical and managerial perspectives within the field. Overall, network visualization underscores the multidimensional and evolving nature of cybersecurity research in SMEs, with strong cross-linkages between risk, innovation, organizational capability, and digital readiness.

Tab. 3: Top 20 most frequently occurring keywords.

KEYWORD	OCCURRENCES	KEYWORD	OCCURRENCES
CYBERSECURITY	69	RISK	13
INFORMATION SECURITY	48	CHALLENGES	12
SMES	47	ADOPTION	11
SME	38	TECHNOLOGY	11
MANAGEMENT	27	INDUSTRY 4 0	10
SECURITY	27	MODEL	10
RISK MANAGEMENT	15	BUSINESS	9
AWARENESS	14	CYBERSECURITY AWARENESS	9
IMPACT	14	INFORMATION	9
CYBER SECURITY	13	INNOVATION	9

Source: Prepared by the authors.

Fig. 3: Co-occurrence network of keywords (2005–2025).



Source: Prepared by the authors.

Influential authors and citation analysis

A critical component of bibliometric assessment is the evaluation of scholarly influence not only through total output and citation counts but also through nuanced metrics, such as the h-index, g-index, m-index, and fractionalized authorship contribution. In the context of cybersecurity and SMEs, these indicators reveal the relative academic weight and trajectory of individual researchers, offering a multidimensional view of intellectual leadership and emerging influence. Among the top contributors, SPRUIT M stands out as the most influential figure in terms of raw citation performance, with 71 total citations across five publications and the highest h-index (5) and g-index (5) in the dataset. With a PY_start of 2016, this indicates sustained scholarly engagement over nearly a decade. His m-index of 0.5 (citational impact normalized by years since first publication) further confirms a steady influence trajectory. His fractionalized contribution (1.31) suggests substantial personal input across co-authored works. Similarly, DE ARROYABE JCF combines a robust citation count (47) with strong bibliometric indices—h-index 4, g-index 5, and a high fractionalized authorship score (1.30)—despite a relatively recent entry into the field (PY_start: 2023). His m-index of 1.33 reflects rapid impact acceleration,

Tab. 4: Top 10 authors by number of citations and by number of documents.

Author	Articles	TC	h_index	g_index	m_index	PY_start	Articles fractionalized
ARRANZ CFA	4	28	3	4	1.5	2024	0.8
ARROYABE MF	4	28	3	4	1.5	2024	0.8
DE ARROYABE JCF	5	47	4	5	1.3333	2023	1.30
GRANDCLAUDON J	4	17	3	4	0.375	2018	1.25
JAYAL A	4	46	3	4	0.6	2021	1.2
LEVY Y	4	6	2	2	0.25	2018	1.33
NCUBUKEZI T	4	8	2	2	0.3333	2020	2.67
PONSARD C	4	17	3	4	0.275	2018	1.25
PRAKASH E	4	46	3	4	0.6	2021	1.2
SPRUIT M	5	71	5	5	0.5	2016	1.31

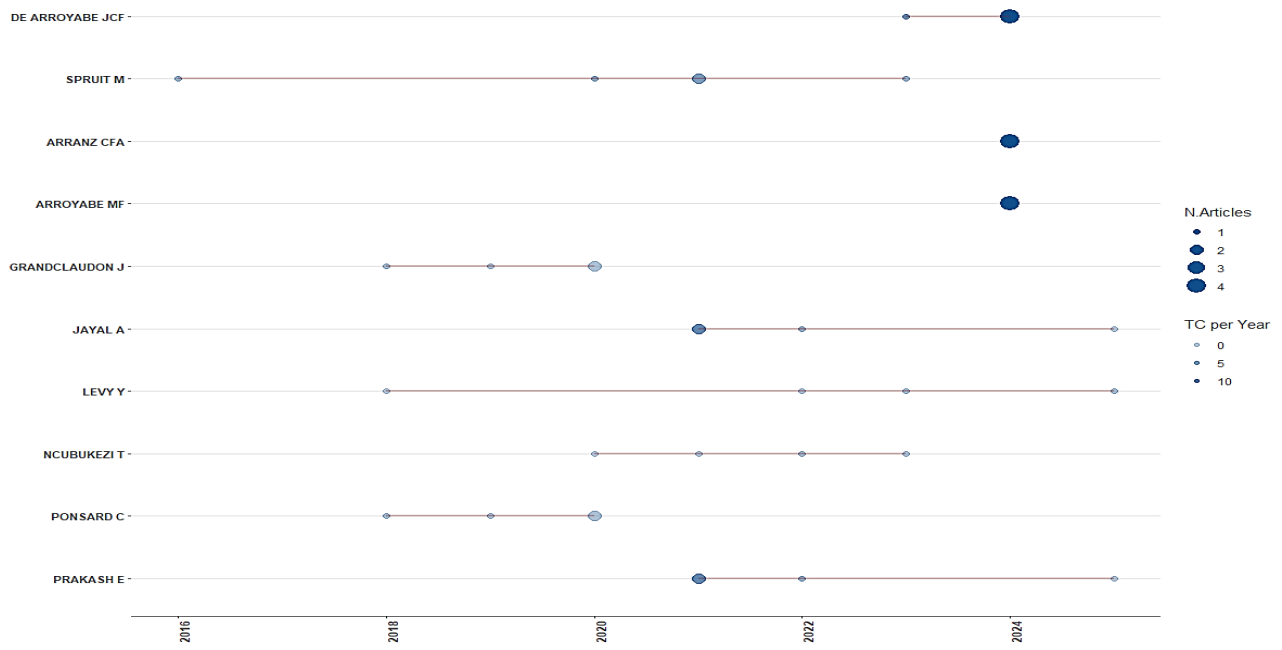
Source: Prepared by the authors.

suggesting that his contributions are not only visible but also gain traction at an impressive rate. The performance profiles of the ARRANZ CFA and ARROYABE MF are identical: each with 4 articles, 28 citations, an h-index of 3, a g-index of 4, and an m-index of 1.5, indicating exceptionally fast citation accumulation since their first publications in 2024. Their fractionalized contributions (0.8) point to balanced collaborative roles, possibly as part of coled or team-based research structures. This unusually high m-index (above 1.0) signals a sharp rise in influence over a very short time span, likely attributable to recent publications in high-visibility outlets or timely topics such as AI, cybersecurity risk in SMEs, or policy-related frameworks. Both JAYAL A and PRAKASH E have 4 articles, 46 citations, and matching h- and g-indices (3 and 4, respectively). Their m-index (0.6) suggests consistent academic engagement since 2021, whereas their fractionalized authorship (1.2) denotes active and possibly leading roles in their research collaborations. They may contribute heavily to applied, managerial, or technical aspects of cybersecurity strategies within SMEs. GRANDCLAUDON J and PONSARD C present similar profiles as methodologically oriented contributors, each with 4 articles, 17 citations, an h-index of 3, and a modest m-index (0.375 and 0.275, respectively). Their PY_start of 2018 suggested that they have maintained moderate, steady scholarly activity over several years. Fractionalized values over 1.2 may hint at primary authorship or fewer co-authors per paper. LEVY Y and NCUBUKEZI T present lower total citation counts (6 and 8, respectively) and h-index values of 2, reflecting early stage or niche influence. Notably, NCUBUKEZI T shows the highest fractionalized authorship (2.67) in the dataset, indicating a disproportionately large personal contribution to their work—potentially as a sole or lead author in smaller teams. However, the m-index values (0.25 and 0.3333) are relatively low, suggesting limited citation momentum thus far.

This author-level analysis provides a richer understanding of influence within the field of SME cybersecurity by incorporating multiple metrics, not just total output or citation volume. Scholars such as SPRUIT M, DE ARROYABE JCF, and the ARRANZ-ARROYABE team emerge as key figures with high academic impact relative to their output and time activity. Their elevated h- and m-indices, especially within recent publishing years, suggest fast-rising trajectories and central roles in shaping emerging discourses. The inclusion of fractionalized authorship adds further clarity to the depth of involvement, distinguishing between lead contributors and those more peripherally involved in co-authored works. Collectively, these insights reinforce the notion of a rapidly evolving research landscape, driven by a mix of established scholars and agile newcomers advancing the frontier of cybersecurity resilience in SMEs.

Lotka's Law provides a theoretical framework for understanding author productivity patterns in the scientific literature. It posits that a majority of authors contribute only one publication to a given field and that the number of authors publishing multiple documents decreases exponentially with the number of publications. The data from the analyzed corpus align closely with this theoretical expectation. Specifically, 91.1% of the authors have authored only one publication, which exceeds the theoretical prediction of 68.3%. This suggests that the research field—cybersecurity in the context of SMEs—is characterized by a high proportion of occasional contributors. These may include scholars from adjacent disciplines or practitioners engaging in collaborative, one-time research efforts. The proportion of authors who have written two (6.5%) or three (1%) documents falls below the theoretical values, and only two authors (0.3%) have published five articles, highlighting the limited presence of highly prolific contributors. This skewed distribution suggests that the field is still emerging and fragmented, lacking a concentrated core of scholars who consistently publish

Fig. 4: Top author productivity over time.



Source: Prepared by the authors.

Tab. 5: Author productivity through Lotka's Law.

Documents written	No. of authors	Proportion of authors	Theoretical
1	717	0.911	0.683
2	51	0.065	0.171
3	8	0.01	0.076
4	9	0.011	0.043
5	2	0.003	0.027

Source: Prepared by the authors.

in this niche area. While interdisciplinary collaboration can be a strength, the absence of a larger group of recurring contributors may hinder the accumulation of deep, specialized knowledge and continuity in theory building. The discrepancy between the observed and theoretical proportions also points to the potential for greater consolidation of expertise. The development of a stronger cohort of dedicated researchers could enhance methodological consistency, strengthen conceptual frameworks, and facilitate long-term research agendas. Overall, the Lotka-based productivity analysis indicates that while the field is drawing broad interest, its intellectual foundation remains diffuse, signaling an opportunity for future scholarly consolidation and leadership.

Geographical distribution of research output and impact

The bibliometric analysis of country-level contributions reveals insightful patterns in global academic production related to cybersecurity within the SME context. The data highlight both the quantity and collaborative nature of research outputs across key contributing nations. The United States ranks first, with 28 publications, representing 11% of the total dataset. The overwhelming

majority (26) are single-country publications, with only two involving international collaboration, resulting in a relatively low multiple-country publication (MCP) ratio of 0.071. This suggests a predominantly domestic research focus, which may reflect strong institutional capabilities and funding mechanisms within the U.S. academic ecosystem that reduce reliance on international co-authorship. Closely following is the United Kingdom with 27 publications (11% frequency), but with a higher degree of international engagement—6 of its publications involve cross-border collaboration, leading to an MCP ratio of 0.222. This underscores the UK's active participation in international cybersecurity networks and research consortia, likely supported by its integration in pan-European research initiatives, particularly in the post-Brexit context, where digital resilience remains a strategic national priority. South Africa ranks third with 15 publications (6%), all of which are single-country outputs, resulting in an MCP ratio of 0. This absence of international co-authorship may reflect a localized research agenda, possibly driven by national policy priorities and institutional independence in cybersecurity development for SMEs.

Both China and Germany contribute 12 publications each (5% frequency), with one internationally co-authored paper per country. Their modest MCP ratios (0.083) point to a relatively self-contained research structure, despite both nations being significant global players in digital infrastructure and innovation. Spain, with 12 publications, also exhibits greater openness to collaboration, with three multicountry outputs and an MCP ratio of 0.25. Australia has the highest level of international collaboration among the top contributors. With 11 publications (4%), 4 are co-authored with foreign institutions, yielding an MCP ratio of 0.364. This suggests a strong strategic orientation toward global research integration, which is consistent with the country's policy alignment toward regional digital cooperation and cyber capacity building. France, Greece, and India each report 7 publications (3% each) but differ notably in collaborative intensity. France has the highest MCP ratio among all listed countries (0.429), with nearly half of its publications involving international partners. Greece and India also display moderate collaboration levels, with an MCP ratio of 0.286. These values highlight the strategic importance of international networks in fostering knowledge exchange and advancing cybersecurity resilience, particularly in regions where SMEs face growing exposure to cyber threats but may lack sufficient domestic support structures.

Collectively, the data reflect a globally dispersed research landscape with notable regional disparities in publication volume and collaborative behavior. Countries such as Australia, the United Kingdom, and France exemplify integrative research ecosystems, whereas others, such as South Africa and the United States, appear to focus more heavily on domestic academic production. These patterns carry implications for future policy and funding strategies, suggesting a need to incentivize broader international research cooperation to address the increasingly transnational nature of cybersecurity threats facing SMEs.

Core publications linking cybersecurity and SMEs

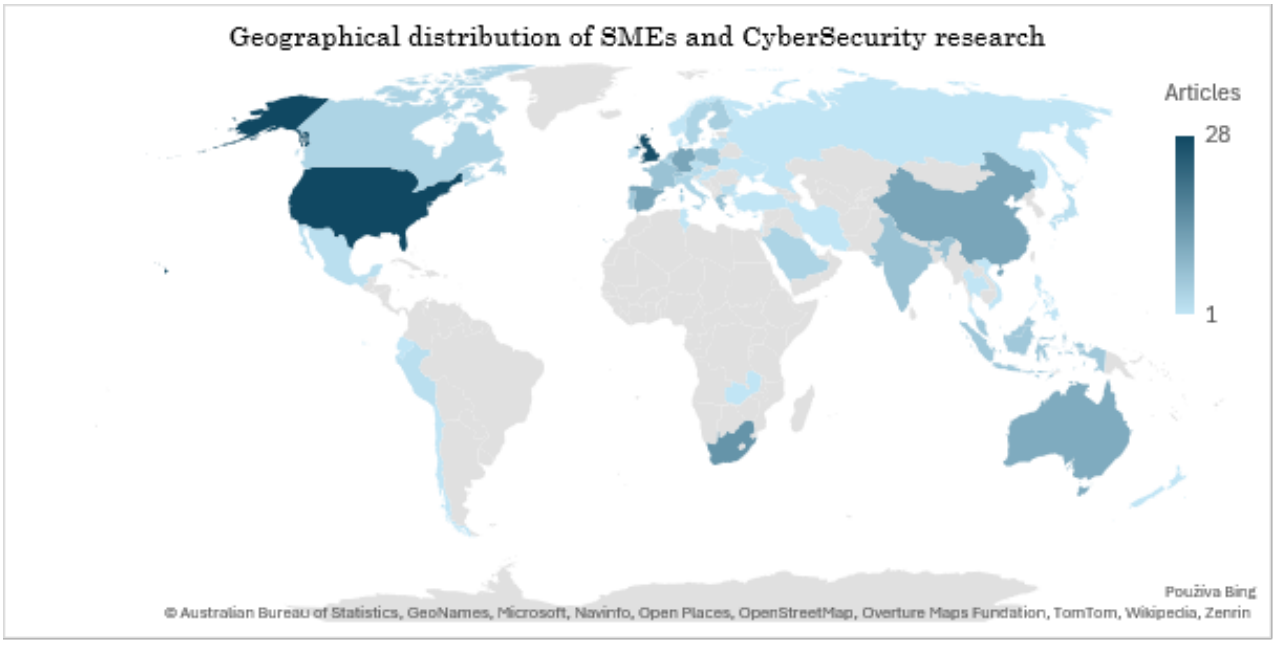
This refined bibliometric overview identifies the most impactful scholarly publications that bridge the intersection of cybersecurity and SMEs, utilizing a combination of total citation count, annual citation performance, and normalized citation rates. These multidimensional indicators offer a more nuanced picture of a publication's influence over time and within its scholarly context. At the forefront is Fielder et al. (2016), with a total of 152 citations, achieving an impressive 15.2 citations per year and a normalized citation count of 8.98. This paper has emerged as a foundational study, shaping the academic discourse on decision-making frameworks and risk-based models in SME cybersecurity. Its high normalized citation score confirms sustained academic attention relative to publication age. Second, Kabanda et al. (2018) garnered 64 citations, with an 8.00 annual rate and a normalized impact of 4.87. Their work, published in a cybersecurity policy context, delves into behavioral and organizational dynamics, emphasizing the importance of SME-specific security practices in developing economies. Yildirim et al. (2011), despite being the oldest publication on the list, maintain relevance, with 63 citations and a steady annual citation rate (4.20). Its normalized TC of 3.99 suggests a consistent long-term impact, reflecting its early contributions to information security management practices tailored to SMEs. Recent publications have also demonstrated strong early influences. Benz et al. (2020) and Heidt et al. (2019) each accumulated over 59–61 citations, with high yearly rates (10.17 and 8.43, respectively), indicating rapid uptake in current academic and practitioner circles. Their research explores innovation resistance, digital transformation challenges, and the integration of cybersecurity into strategic business models for SMEs. Notably, Kljucnikov et al. (2019), representing Central and Eastern Europe, provide a regionally grounded perspective on cybersecurity readiness, earning 55 citations and maintaining a solid normalized citation rate of 4.91, signaling cross-regional relevance. Among the newest entries, Tamvada (2022) and Wong et al. (2022) show remarkable momentum, with over 13 citations

Tab. 6: The number and share of individual countries involved in publication activities focused on cybersecurity in SMEs.

Country	Articles	Freq	Single-country publication	Multiple-country publication	MCP ratio
The United States	28	0.11	26	2	0.071
The United Kingdom	27	0.11	21	6	0.222
South Africa	15	0.06	15	0	0
China	12	0.05	11	1	0.083
Germany	12	0.05	11	1	0.083
Spain	12	0.05	9	3	0.25
Australia	11	0.04	7	4	0.364
France	7	0.03	4	3	0.429
Greece	7	0.03	5	2	0.286
India	7	0.03	5	2	0.286

Source: Prepared by the authors.

Fig. 5: Geographical distribution of SME and cybersecurity research.



Source: Prepared by the authors.

per year, despite their short citation window. Their research highlights SME preparedness in the face of disruptive technologies and evolving cyber threats, offering early signs of becoming future landmark studies. Gupta (2018) and Armenia (2021) round out the top 10 with 51 and 50 citations, respectively. Both studies focus on change management and simulation modeling for cyber risk, with balanced performance across all indicators. In conclusion, this set of publications forms the intellectual backbone of SME-focused cybersecurity literature. While citation counts alone offer initial insights, integrating time-adjusted metrics such as citations per year and normalized citation rates helps identify not only which articles are most referenced but also which ones shape the current

Tab. 7: Top 10 publications by number of citations.

Author and year	DOI	Total citations	TC per year	Normalized TC
FIELDER A, 2016	10.1016/j.dss.2016.02.012	152	15.20	8.98
KABANDA S, 2018	10.1080/10919392.2018.1484598	64	8.00	4.87
YILDIRIM EY, 2011	10.1016/j.ijinfomgt.2010.10.006	63	4.20	3.99
BENZ M, 2020	10.1016/j.bushor.2020.03.010	61	10.17	5.73
HEIDT M, 2019	10.1007/s10796-019-09959-1	59	8.43	5.27
KLJUCNIKOV A, 2019	10.9770/jesi.2019.6.4(37)	55	7.86	4.91
TAMVADA JP, 2022	10.1016/j.techfore.2022.122088	55	13.75	4,25
WONG LW, 2022	10.1016/j.ijinfomgt.2022.102520	53	13.25	4,09
GUPTA S, 2018	10.1108/JOCM-06-2017-0230	51	6.38	3.88
ARMENIA S, 2021	10.1016/j.dss.2021.113580	50	10.00	4.86

Source: Prepared by the authors.

and future academic narrative. These works underscore the field's transition from exploratory analysis to applied, strategy-oriented research, especially within the rapidly evolving risk landscape of SMEs.

Leading journals in SME cybersecurity research

This extended performance assessment offers deeper bibliometric insight into the scholarly venues contributing to cybersecurity research in the context of small and medium-sized enterprises (SMEs). In contrast to traditional counts of articles or citations alone, the following analysis integrates composite metrics—the h-index, g-index, m-index, and publication onset (PY_start)—to reflect not only productivity and impact but also the temporal consistency and citation velocity of each source. At the top of the list is Information and Computer Security, with 10 articles, a total citation count (TC) of 94, and an h-index of 5—making it the most consistently cited journal in this collection. Its g-index of 9 and m-index of 0.5 suggest a reliable and steady academic contribution to the SME cybersecurity discourse since 2016, particularly in terms of organizational security strategies and data protection frameworks tailored to SMEs. Next, the Journal of Computer Information Systems has published 4 articles that together amassed 52 citations, with an h-index and g-index of 4. This journal, which has also been active since 2016, plays a notable role in information management and business systems, offering a blend of technical and managerial perspectives relevant for SMEs adapting to cybersecurity challenges. The ARES Conference (2021)—a prominent venue focused on Availability, Reliability, and Security—shows impressive engagement, with 4 papers, 18 citations, and an h-index of 3. Despite its recent entry in 2021, its m-index of 0.6 reflects rapid citation activity, underlining its role in fostering discussion on applied and emerging topics in SME cybersecurity. *Computers & Security*, a discipline-focused journal, follows with 5 articles and 43 citations, establishing a solid h-index of 3 and a relatively high m-index of 0.75, the highest among all sources. This suggests not only the technical credibility of this journal but also its current relevance, with all included articles published since 2022—making it a key emerging source for high-impact research. IEEE Access, known for its open-access model and rapid dissemination, contributed 4 articles and 77 citations, with a g-index of 4 and an m-index of 0.5. Although more generalist in scope, its large and multidisciplinary audience supports fast visibility for SME-focused cybersecurity research, especially at the systems and infrastructure level. Technological forecasting and social change, with 3 papers and 86 citations, maintains a g-index of 3 and a healthy m-index of 0.6, indicating that forward-looking studies on cybersecurity and SME resilience are gaining traction. The journal's orientation toward innovation, foresight, and strategic planning makes it particularly suitable for long-term digital transformation narratives. Several conference proceedings are also influential. Notably, the IEEE CAMAD 2019 Workshop and the ITMS 2020 Conference each contributed 2 papers with moderate citation counts (14 and 12, respectively). Both show h-index values of 2 and m-indices above 0.28, indicating consistent engagement within focused research communities related to network design and digital systems in SMEs. The journal *Computers*, with 3 articles and 35 citations, combines technical depth

Tab. 8: Top 10 journals.

Sources	Articles	TC	H-index	G-index	M-index	PY_start
Information and Computer Security	10	94	5	9	0.5	2016
Journal of Computer Information Systems	4	52	4	4	0.4	2016
Ares 2021: 16th International Conference on Availability, Reliability and Security	4	18	3	4	0.6	2021
Computers & Security	5	43	3	5	0.75	2022
IEEE Access	4	77	3	4	0.5	2020
Technological Forecasting and Social Change	3	86	3	3	0.6	2021
2019 IEEE 24th International Workshop on Computer Aided Modeling and Design Of Communication Links and Networks (IEEE CAMAD)	2	14	2	2	0.286	2019
2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)	2	12	2	2	0.333	2020
Computers	3	35	2	3	0.4	2021
Decision Support Systems	2	202	2	2	0.2	2016

Source: Prepared by the authors.

with practical applicability, sustaining a g-index of 3 and an m-index of 0.4 since 2021. Finally, Decision Support Systems stands out for their extraordinary citation impact: while only 2 articles were published, they generated 202 citations, achieving the highest citation density of all venues. Although the m-index is relatively low (0.2) because it started earlier in 2016, the data suggest that the contributions presented here are foundational or highly influential and are often cited in theoretical and policy-level research on strategic cybersecurity decision-making.

This analysis reveals that SME cybersecurity research is being disseminated across a diverse spectrum of journals and conferences, spanning domains such as information security, digital innovation, business systems, and technical engineering. The inclusion of both long-standing academic journals and emerging high-impact conferences indicates that the field is maturing and becoming increasingly interdisciplinary. Importantly, metrics such as the m-index and g-index help identify not only where research is published but also where it is gaining sustained and growing influence—an essential factor in strategic publication planning and knowledge dissemination.

The Role of Public Policy in SME Cybersecurity

The bibliometric findings revealed that several highly cited studies indirectly address the influence of public policy and regulation on cybersecurity practices in small and medium-sized enterprises (SMEs). For instance, Kabanda et al. (2018) examined cybersecurity behaviors in developing economies, emphasizing that the absence of clear regulatory frameworks and limited institutional support hinder the implementation of even basic security controls. Their study underscores that regulatory guidance and government-backed awareness programs are crucial for cultivating cybersecurity readiness among resource-constrained firms. Similarly, Heidt et al. (2019) discussed the governance dimension of digital transformation, highlighting that compliance requirements, such as those derived from the General Data Protection Regulation (GDPR), serve as external drivers compelling SMEs to adopt structured cybersecurity practices. In Central and Eastern Europe, Kljucnikov et al. (2019) found that the adoption of cybersecurity standards remains uneven largely due to weak national coordination mechanisms and insufficient financial incentives for small businesses. These observations align with Tamvada et al. (2022), who demonstrated that the successful adoption of Industry 4.0 technologies in emerging economies depends not only on technological readiness but also on the existence of enabling public policies that promote security capacity building.

These bibliometric insights collectively indicate that the regulatory and policy environment acts as a decisive external enabler or barrier to cybersecurity maturity within SMEs. In the European context, several policy instruments have redefined this environment. The NIS2 Directive (EU 2022/2555) expands the obligations of member states to strengthen national cybersecurity capacities and explicitly addresses supply chain dependencies, which indirectly affect SMEs participating in critical sectors. The Cyber Resilience Act (2024) further extends these responsibilities by imposing security-by-design and postmarket surveillance requirements on producers of digital products and software components. These frameworks not only elevate baseline security expectations but also encourage SMEs to align their internal processes with harmonized European standards.

At the national level, strategies such as the National Cybersecurity Strategy of the Slovak Republic 2021–2025 provide the domestic translation of EU-level priorities. They introduce instruments for SME support, including education initiatives, sectoral training programs, and partnerships with academia. However, empirical studies and ENISA reports (2025) reveal persistent gaps in awareness and the practical implementation of these measures. Many SMEs remain unaware of available state support or consider compliance too complex and costly, which leads to a regulatory divide between large enterprises and smaller actors. The same issue was identified in the bibliometric corpus, where studies emphasize that information asymmetry and limited administrative capacity prevent SMEs from effectively leveraging policy frameworks (Uchendu et al., 2021; Carrapico & Barrinha, 2017). Public institutions such as ENISA and national CSIRT centers, therefore, play a critical intermediary role. By providing simplified guidelines, online risk assessment tools, and funding schemes under the EU Digital Europe Program, they help translate regulatory intent into practical actions. Yet, the bibliometric evidence also indicates that awareness of these initiatives remains low, suggesting that the effectiveness of public policy depends on its accessibility and contextualization for SMEs. From a conceptual standpoint, the interplay between regulation and organizational behavior can be interpreted through the lens of institutional theory, where coercive pressures (legal compliance), normative pressures (industry expectations), and mimetic pressures (peer imitation) collectively shape SME cybersecurity adoption. Effective public policy must, therefore, balance prescriptive regulation with supportive capacity-building measures. In line with the formulated Research Question, future research should assess to what extent European and national policy instruments genuinely enhance cybersecurity resilience at the firm level and how these mechanisms can be optimized to support SMEs within an integrated, multilevel governance system.

DISCUSSION

This study provided a systematic bibliometric overview of the development of cybersecurity research in the context of small and medium-sized enterprises (SMEs) between 2005 and 2025. The findings indicate a clear increase in academic interest in this topic, which can be attributed to the growing digitalization of SMEs, the emergence of Industry 4.0 technologies, and the increasing vulnerability of SMEs to cyber threats. This discussion interprets the main findings in light of theoretical frameworks, practical implications, and future research opportunities.

Interpretation of key findings

The results demonstrate a consistent increase in the volume of research dedicated to cybersecurity in SMEs, with an average annual growth rate of 16.7%. This trend aligns with the rising number of cyber incidents targeting SMEs, as well as regulatory initiatives aimed at strengthening digital security (e.g., NIS2, GDPR). Keyword analysis confirmed a shift in research focus from purely technical aspects (e.g., firewalls, encryption) to strategic and behavioral approaches (e.g., cybersecurity awareness, risk management, digital literacy). This development reflects a broader understanding of cybersecurity as a socio-technical phenomenon. Notably, terms such as “awareness,” “training,” and “governance” were frequently associated with SMEs, indicating a growing emphasis on practical and organizationally embedded solutions. In addition, bibliometric evidence suggests an increasing recognition of the role of public policy and regulation as external drivers of SME cybersecurity maturity. Studies frequently referenced frameworks such as the EU NIS2 Directive, the Cyber Resilience Act (2024), and GDPR, highlighting how compliance obligations, national strategies, and EU-level initiatives act as catalysts for organizational change. This reflects a research trend where cybersecurity in SMEs is not viewed solely as a managerial or technical challenge but also as a governance and policy issue shaped by multilevel regulatory environments.

Geographical analysis revealed dominance by countries such as the United States and the United Kingdom in terms of absolute publication volume, while countries like France and Australia demonstrated high levels of international collaboration. Cybersecurity research in SMEs is, therefore, not only technically diverse but also globally distributed, pointing to the need for context-sensitive strategies. The application of Lotka's Law revealed that most authors contributed only one publication to the field, which suggests a fragmented research community. This fragmentation presents an opportunity for the consolidation of the field through the formation of stable research networks and collaborative working groups.

Limitations of the evidence base

While the bibliometric method provides a robust and transparent overview of the development of a research field, it also has limitations. First, the analysis was based exclusively on the Web of Science database. Although this ensures a high quality of included publications, it excludes relevant studies from other databases, such as Scopus, IEEE Xplore, and Google Scholar, which could lead to a partial view of the topic. Second, the search string and keyword selection may have influenced the scope of the included documents. Although the search strategy was systematic and designed to reflect thematic variation, a degree of selection bias cannot be ruled out. Third, bibliometric analysis relies primarily on quantitative indicators and cannot capture the depth, quality, or contextual significance of individual publications. For instance, a high citation count does not necessarily imply positive impact or methodological rigor. Finally, given that the review includes studies published through mid-2025, recently published articles may not yet have accumulated sufficient citations to reflect their influence, which may skew impact-related metrics.

Comparison with existing literature

The findings of this study are consistent with previous research that confirms the vulnerability of SMEs to cyber threats and the need for more than just technical solutions (e.g., Bada & Nurse, 2019; Uchendu et al., 2021). However, this study extends the literature by mapping thematic clusters and dominant discourse lines through bibliometric network analysis (e.g., security standards, gamification, ISO 27001). The thematic focus of publications has clearly evolved. Older studies concentrated on basic threats (e.g., viruses, data protection), while more recent work emphasizes resilience models, employee training, and security culture. This indicates maturation of the research field. This study also confirms the absence of standardized frameworks tailored to SMEs, as highlighted by organizations like ENISA. On the other hand, studies such as Tamvada et al. (2022) demonstrate regional disparities in the implementation of Industry 4.0 among SMEs, which is mirrored in the geographical distribution of literature.

Implications for research, practice, and policy

From a research perspective, this study advocates greater interdisciplinary collaboration among technical, managerial, and behavioral sciences. Future research should prioritize longitudinal studies to evaluate the effectiveness of cybersecurity awareness interventions and training programs in SMEs. It is also essential to develop regional cybersecurity preparedness indices tailored specifically for small firms. In terms of practice, the study supports the use of gamified tools (e.g., CySecEscape 2.0) and scalable training models for raising cybersecurity awareness among employees. Organizations can use the findings to select appropriate standards and frameworks that are realistically implementable in the SME context. Policy implications include the need to harmonize cybersecurity regulations and provide support mechanisms for smaller businesses that face compliance requirements without adequate resources. Simplified ISO 27001 implementation methodologies, GDPR compliance guidelines for SMEs, and the public funding of educational tools can help enhance the resilience of the digital SME sector. In conclusion, this bibliometric analysis contributes to the understanding of the intellectual, geographical, and thematic structure of cybersecurity research in SMEs and provides a foundation for evidence-based, context-aware strategies aimed at improving digital resilience in this vital economic sector.

Cent. Eur. J. Public Policy 2025; 19(2): 87-110
DOI: 10.2478/cejpp-2025-0010

CONCLUSION

This bibliometric study underscores the increasing scholarly attention given to cybersecurity within the specific context of small and medium-sized enterprises (SMEs). An analysis of 245 peer-reviewed documents published between 2005 and 2025 reveals the thematic complexity and interdisciplinary nature of this evolving research area. The findings highlight a growing academic consensus that cybersecurity in SMEs is not merely a technical issue but a multidimensional challenge encompassing strategic, organizational, behavioral, and technological dimensions. Keyword co-occurrence analysis revealed a notable shift from narrowly defined technical concerns to a broader framing of cybersecurity. Terms such as "information security," "risk management," "awareness," and "digital transformation" frequently co-occurred with SME-specific terminology, suggesting a research agenda that acknowledges the constraints and operational realities of small firms. This shift aligns with a more holistic approach to cyber resilience, which integrates human-centric design, strategic alignment, and technological innovation. Moreover, the bibliometric evidence indicates that public policy and regulatory frameworks constitute an additional but often overlooked dimension of SME cybersecurity. Several highly cited studies, including Kabanda et al. (2018), Heidt et al. (2019), Kljucnikov et al. (2019), and Tamvada et al. (2022), implicitly confirm that the presence or absence of effective regulatory and institutional support directly affects the cybersecurity capacity of small firms. Their findings collectively highlight that state-led strategies, funding programs, and compliance frameworks play a pivotal role in shaping cybersecurity behavior, particularly in resource-constrained environments. The co-occurrence mapping also revealed distinct yet interconnected clusters that represent the intellectual structure of the field. These clusters include governance, cybersecurity training, Industry 4.0 readiness, and standardization frameworks. The presence of such clusters indicates conceptual convergence around priority areas such as scalable awareness programs, the implementation of cybersecurity standards, and innovation-driven risk mitigation strategies. Notably, concepts such as ISO 27001, GDPR compliance, and gamified training tools (e.g., CySecEscape 2.0) reflect a transition toward practical, solution-oriented research. The regulatory and policy dimension further reinforces this evolution, as European instruments like the NIS2 Directive (EU 2022/2555), the Cyber Resilience Act (2024), and national cybersecurity strategies increasingly emphasize SME inclusion and capacity building. These frameworks contribute to harmonized standards, reduce information asymmetry, and provide institutional mechanisms, such as ENISA guidance, CSIRT networks, and Digital Europe Programme grants, which enable smaller enterprises to operationalize cybersecurity in practice. The analysis of author productivity through Lotka's Law revealed that the field remains fragmented, with a significant proportion of authors contributing only once. While this fragmentation presents challenges in building cohesive academic networks, it also reflects the broad interest across disciplines and countries. Strengthening longitudinal research efforts and fostering stable, interdisciplinary research collaborations could facilitate thematic consolidation and enhance knowledge integration. Geographically, the bibliometric analysis revealed that research is globally distributed, with the United States and the United Kingdom leading in terms of publication volume. Countries such as Australia, France, Spain, and South Africa showed notable contributions and relatively high levels of international collaboration. This global dispersion reinforces the universal relevance of SME cybersecurity and the importance of context-sensitive approaches that consider regional disparities in technological maturity, regulatory frameworks, and institutional support. Citation and journal impact metrics further confirm the interdisciplinary nature of the field. Influential research appears in both technical and managerial journals, indicating that SME cybersecurity is being approached from multiple vantage points. High-impact contributions emphasize the importance of cybersecurity culture, regulatory adaptation, and organizational preparedness, highlighting the intersection of policy, practice, and innovation. Integrating these insights, this study suggests that effective SME cybersecurity cannot be achieved through technological innovation alone, and it requires coherent public policies that translate regulatory intent into accessible support for small firms. Future research should, therefore, explore the interaction between organizational readiness and national or EU-level governance mechanisms to identify which policy configurations most effectively foster SME cyber resilience. From a strategic perspective, the findings underscore the urgent need for tailored cybersecurity solutions for SMEs. Given their resource constraints, SMEs require lightweight, scalable, and context-appropriate interventions. These might include simplified compliance guides, modular training platforms, and public-private partnerships to support knowledge transfer. Moreover, regulatory bodies should consider differentiated cybersecurity policies that reflect the specific capabilities and limitations of SMEs. This study also highlights key research gaps and future directions. There is a need for more empirical evidence on the effectiveness of cybersecurity interventions in SME contexts, particularly those that address human factors, strategic decision-making, and digital capability development. Longitudinal and comparative studies across regions and sectors could also provide deeper insights into resilience patterns and best practices. Ultimately,

the integration of bibliometric evidence with the policy dimension offers a more comprehensive understanding of SME cybersecurity as both a technological and institutional phenomenon. The alignment of academic insights with evolving public policy through instruments such as NIS2, the Cyber Resilience Act, and national strategies creates a pathway toward evidence-based policymaking that supports inclusive and sustainable digital resilience among Europe's SMEs. In conclusion, this bibliometric analysis maps the conceptual, thematic, and geographical landscape of cybersecurity research in SMEs. The growing scholarly engagement reflects the recognition that the cyber resilience of SMEs is essential to the broader stability and security of digital economies. By identifying dominant trends, influential contributors, and thematic gaps, this study provides a foundation for evidence-based policymaking, targeted research funding, and the development of integrated, human-centered cybersecurity strategies tailored to the needs of small and medium-sized enterprises in an increasingly complex and adversarial digital environment.

FUNDING

This work was supported by the Slovak Research and Development Agency under the contract no. VV-MVP-24-0272.

DECLARATION OF COMPETING INTEREST

The authors hereby declare no conflicts of interest.

CONSENT FOR PUBLICATION

The authors are willing for publication of this manuscript.

DATA AVAILABILITY

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

AUTHORS' CONTRIBUTIONS

CRediT: **Matúš Panko**: conceptualization, methodology, software, writing—original draft. **Leoš Šafár**: conceptualization, data curation, formal analysis, writing—review and editing. **Michal Mešťan**: formal analysis, writing—review and editing.

GENERATIVE AI STATEMENT

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

Tab. 9: PRISMA 2020 Checklist.

Section and topic	Item #	Checklist item	Location where item is reported
TITLE			
Title	1	Identify the report as a systematic review.	Title page, abstract
ABSTRACT			
Abstract	2	See the PRISMA 2020 for Abstract checklist.	Abstract section
INTRODUCTION			
Rationale	3	Describe the rationale for the review in the context of existing knowledge.	Introduction section
Objectives	4	Provide an explicit statement of the objective(s) or question(s) the review addresses.	Introduction section
METHODS			
Eligibility criteria	5	Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses.	Methods—eligibility criteria
Information sources	6	Specify all databases, registers, websites, organizations, reference lists, and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted.	Methods—information sources (Web of Science, search completed June 2025)
Search strategy	7	Present the full search strategies for all databases, registers, and websites, including any filters and limits used.	Methods—search strategy (keywords, filters)
Selection process	8	Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the process.	Methods—selection process (screening by document type, language, subject area)
Data collection process	9	Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process.	Methods—data collection (using Bibliometrix in RStudio)
Data items	10a	List and define all outcomes for which data were sought. Specify whether all results that were compatible with each outcome domain in each study were sought (e.g., for all measures, time points, analyses), and if not, the methods used to decide which results to collect.	Methods—keyword analysis, citation metrics, co-authorship networks
	10b	List and define all other variables for which data were sought (e.g., participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information.	Methods—additional metadata (publication year, country, document type)
Study risk of bias assessment	11	Specify the methods used to assess risk of bias in the included studies, including details of the tool(s) used, how many reviewers assessed each study and whether they worked independently, and if applicable, details of automation tools used in the process.	Not applicable—no risk of bias assessment conducted
Effect measures	12	Specify for each outcome the effect measure(s) (e.g., risk ratio, mean difference) used in the synthesis or presentation of results.	Not applicable—no effect size or outcome comparison
Synthesis methods	13a	Describe the processes used to decide which studies were eligible for each synthesis (e.g., tabulating the study intervention characteristics and comparing against the planned groups for each synthesis [item #5]).	Methods—descriptive bibliometric synthesis using Bibliometrix
	13b	Describe any methods required to prepare the data for presentation or synthesis, such as handling of missing summary statistics, or data conversions.	Methods—descriptive bibliometric synthesis using Bibliometrix
	13c	Describe any methods used to tabulate or visually display results of individual studies and syntheses.	Methods—descriptive bibliometric synthesis using Bibliometrix
	13d	Describe any methods used to synthesize results and provide a rationale for the choice(s). If meta-analysis was performed, describe the model(s) and method(s) to identify the presence and extent of statistical heterogeneity and software package(s) used.	Methods—descriptive bibliometric synthesis using Bibliometrix

Continued **Tab. 9:** PRISMA 2020 Checklist.

Section and topic	Item #	Checklist item	Location where item is reported
Synthesis methods	13e	Describe any methods used to explore possible causes of heterogeneity among study results (e.g., subgroup analysis, meta-regression).	Methods—descriptive bibliometric synthesis using Bibliometrix
	13f	Describe any sensitivity analyses conducted to assess robustness of the synthesized results.	Methods—descriptive bibliometric synthesis using Bibliometrix
Reporting bias assessment	14	Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases).	Not applicable—bibliometric study
Certainty assessment	15	Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome.	Not applicable
RESULTS			
Study selection	16a	Describe the results of the search and selection process from the number of records identified in the search to the number of studies included in the review, ideally using a flow diagram.	Results—study selection, flow of inclusion (n = 286 → 245)
	16b	Cite studies that might appear to meet the inclusion criteria, but which were excluded, and explain why they were excluded.	Methods—list of exclusion criteria (e.g., language, document type, topic mismatch)
Study characteristics	17	Cite each included study and present its characteristics.	Results—core publications, tables with citation data
Risk of bias in studies	18	Present assessments of risk of bias for each included study.	Not applicable
Results of individual studies	19	For all outcomes, present, for each study: (a) summary statistics for each group (where appropriate) and (b) an effect estimate and its precision (e.g., confidence/credible interval), ideally using structured tables or plots.	Not applicable—no meta-analysis or comparative statistics
Results of syntheses	20a	For each synthesis, briefly summarize the characteristics and risk of bias among contributing studies.	Results—descriptive synthesis of themes, authors, journals
	20b	Present results of all statistical syntheses conducted. If meta-analysis was done, present for each the summary estimate and its precision (e.g., confidence/credible interval) and measures of statistical heterogeneity. If comparing groups, describe the direction of the effect.	Results—descriptive synthesis of themes, authors, journals Results—descriptive synthesis of themes, authors, journals
	20c	Present results of all investigations of possible causes of heterogeneity among study results.	Results—descriptive synthesis of themes, authors, journals
	20d	Present results of all sensitivity analyses conducted to assess the robustness of the synthesized results.	Results—descriptive synthesis of themes, authors, journals
Reporting biases	21	Present assessments of risk of bias due to missing results (arising from reporting biases) for each synthesis assessed.	Not applicable
Certainty of evidence	22	Present assessments of certainty (or confidence) in the body of evidence for each outcome assessed.	Not applicable
DISCUSSION			
Discussion	23a	Provide a general interpretation of the results in the context of other evidence.	Discussion—synthesis with prior literature
	23b	Discuss any limitations of the evidence included in the review.	Discussion—thematic and dataset limitations
	23c	Discuss any limitations of the review processes used.	Discussion—limitations of bibliometric method (e.g., database dependence)
	23d	Discuss implications of the results for practice, policy, and future research.	Discussion—recommendation section

Continued **Tab. 9:** PRISMA 2020 Checklist.

Section and topic	Item #	Checklist item	Location where item is reported
OTHER INFORMATION			
Registration and protocol	24a	Provide registration information for the review, including register name and registration number, or state that the review was not registered.	Review not registered
	24b	Indicate where the review protocol can be accessed, or state that a protocol was not prepared.	No protocol was prepared
	24c	Describe and explain any amendments to information provided at registration or in the protocol.	Not applicable
Support	25	Describe sources of financial or nonfinancial support for the review and the role of the funders or sponsors in the review.	Funding
Competing interests	26	Declare any competing interests of review authors.	Declarations—no conflict of interest
Availability of data, code, and other materials	27	Report which of the following are publicly available and where they can be found: template data collection forms, data extracted from included studies, data used for all analyses, analytic code, and any other materials used in the review.	Available upon request or documented in Methods

Source: Prepared by the authors, based on the PRISMA 2020 Checklist.

REFERENCES

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy, 1*(2), 219–238. https://doi.org/10.3390/jcp1020012

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

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2020). Cyber resilience progression model. *Applied Sciences, 10*(21), 7393. https://doi.org/10.3390/app10217393

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber)security actor? *JCMS: Journal of Common Market Studies, 55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575

European Union Agency for Cybersecurity. (2025, May 8). *Cybersecurity for SMEs – Challenges and recommendations*. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Gupta, J.; Barzotto, M.; Khorasgani, A. Does Size Matter in Predicting SMEs Failure? Int. J. Fin. Econ. 2018, 23, 571–605. https://doi.org/10.1002/ijfe.1638

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security gap between SMEs and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers, 21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kljucnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: Factors of success. *Entrepreneurship and Sustainability Issues, 6*(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Linnenluecke, M. K., Marrone, M., & Singh, A. K. (2019). Conducting systematic literature reviews and bibliometric analyses. *Australian Journal of Management.* https://doi.org/10.1177/0312896219877678

Löffler, E., Schneider, B., Zanwar, T., & Asprion, P. M. (2021). CySecEscape 2.0—A virtual escape room to raise cybersecurity awareness. *International Journal of Serious Games, 8*(1), 59–70. https://doi.org/10.17083/ijsg.v8i1.413

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

Passas, I. (2024). Bibliometric analysis: The main steps. *Encyclopedia, 4*(2), 1014–1025. https://doi.org/10.3390/encyclopedia4020065

Ponemon Institute. The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud; Ponemon Institute: North Traverse City, MI, USA, 2023.

Tamvada, J. P., Narula, S., Audretsch, D., Puppala, H., & Kumar, A. (2022). Adopting new technology is a distant dream? The risks of implementing Industry 4.0 in emerging economy SMEs. *Technological Forecasting and Social Change, 185*, 122088. https://doi.org/10.1016/j.techfore.2022.122088

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Westerlund, M. (2020). Digitalization, internationalization and scaling of online SMEs. *Technology Innovation Management Review, 10*(4), 48–57. https://doi.org/10.22215/timreview/1346