FESIDE
Fundación Emilio Soldevilla
para la Investigación y Desarrollo
de la Economía de la Empresa

enpresa institutua
Instituto de Economía Aplicada a la Empresa

Management Letters / Cuadernos de Gestión

journal homepage: https://ojs.ehu.eus/index.php/CG
ISSN: 1131-6837 / e-ISSN: 1988-2157

Research on cybersecurity and business: A bibliometric review (2004-2023)

Investigación en ciberseguridad y negocios: una revisión bibliométrica (2004-2023)

Luciano Barcellos-Paula*, Anna M. Gil-Lafuente[a], José M. Merigó[b]

[a] *Department of Business Administration, University of Barcelona, Av. Diagonal 690, 08034 Barcelona, Spain – amgil@ub.edu – https://orcid.org/0000-0003-0905-3929*

[b] *Faculty of Engineering and Information Technology, University of Technology Sydney, 81 Broadway, Ultimo 2007, NSW, Australia – jose.merigo@uts.edu.au – https://orcid.org/0000-0002-4672-6961*

* ***Corresponding author:*** *CENTRUM Católica Graduate Business School, Pontificia Universidad Católica del Perú. Calle Daniel Alomía Robles 125-129, Los Álamos de Monterrico, Santiago de Surco, Lima 33, Peru – lbarcellosdepaula@pucp.edu.pe – https://orcid.org/0000-0003-4249-0565*

ARTICLE INFO

Received 21 September 2024,
Accepted 20 February 2025

Available online 21 March 2025

DOI: 10.5295/cdg.242288lb

JEL: M10, M15

ABSTRACT

Cybersecurity poses a significant risk for companies due to the rise in cyberattacks worldwide, leading to increased uncertainty in security management and putting the sustainability of businesses at risk. Despite some academic contributions, limited bibliometric studies on integrating cybersecurity and business information exist. The research aims to assist academics, policymakers, and decision-makers in cybersecurity management. The authors conducted a bibliometric review using scientific mapping and performance analysis. The study used the Web of Science database and Bibliometrix software to analyze 410 articles and 1,355 authors across nine bibliometric indicators between 2004 and 2023. This article is novel in proposing a bibliometric review of cybersecurity and business, as the other studies addressed specific sectors and do not allow for an integrated view of information on these two topics. The main findings showed an annual growth of 27.63% and an international co-authorship of 31.46%. The United States of America has the highest scientific production, followed by the United Kingdom and China. Business Horizons and IEEE Access are the most influential journals in this field of research. This study can improve the analysis of academics, policymakers, and decision-makers in companies regarding security management. Future studies could propose management models to improve cybersecurity in organizations.

Keywords: Cybersecurity, Business, Safety Management, Scientific Mapping, risk, Bibliometrix.

RESUMEN

La ciberseguridad representa un riesgo importante para las empresas debido al aumento de los ciberataques en todo el mundo, lo que genera una mayor incertidumbre en la gestión de la seguridad y pone en riesgo la sostenibilidad de las empresas. A pesar de algunas contribuciones académicas, existen estudios bibliométricos limitados sobre la integración de la ciberseguridad y la información empresarial. La investigación tiene como objetivo ayudar a los académicos, los responsables políticos y los tomadores de decisiones en la gestión de la ciberseguridad. Los autores realizaron una revisión bibliométrica utilizando el mapeo científico y el análisis de rendimiento. El estudio utilizó la base de datos Web of Science y el software Bibliometrix para analizar 410 artículos y 1,355 autores en nueve indicadores bibliométricos entre 2004 y 2023. Este artículo es novedoso al proponer una revisión bibliométrica de la ciberseguridad y los negocios, ya que los otros estudios abordaron sectores específicos y no permiten una visión integrada de la información sobre estos dos temas. Los principales hallazgos mostraron un crecimiento anual del 27.63% y una coautoría internacional del 31.46%. Los Estados Unidos de América cuentan con la mayor producción científica, seguido de Reino Unido y China. Business Horizons e IEEE Access son las revistas más influyentes en este campo de investigación. Este estudio puede mejorar el análisis de académicos, formuladores de políticas y tomadores de decisiones en las empresas en relación con la gestión de la seguridad. Estudios futuros podrían proponer modelos de gestión para mejorar la ciberseguridad en las organizaciones.

Palabras clave: Ciberseguridad, Negocios, Gestión de la seguridad, Mapeo científico, Riesgo, Bibliometrix

1. INTRODUCTION

Cybersecurity is a critical risk for companies due to the increase in cyberattacks in various parts of the world (Bresniker *et al.*, 2019), which increases uncertainty in the process of managing it and, in turn, jeopardizes the sustainability of their businesses (Kosmowski *et al.*, 2022). Despite academic contributions, there are few bibliometric studies on cybersecurity and business. For example, a study dedicated to the healthcare sector provided an overview of the literature on the intersection of cybersecurity and healthcare (Jalali *et al.*, 2019). Key findings revealed that cyber vulnerabilities are not all digital and that physical threats contribute to breaches and impact the physical safety of patients (Jalali *et al.*, 2019). In another study, researchers conducted a bibliometric review of research on autonomous vessels' risk, safety, and reliability, and it confirmed the relevance of further cybersecurity risk analyses (Chaal *et al.*, 2023). Other researchers conducted a systematic literature review, not a bibliometric review, to analyze cybersecurity awareness in the industrial Internet of Things (IoT) context (Corallo *et al.*, 2022). In this case, the study analyzed 23 articles in four areas of analysis. In short, the studies presented use bibliometric or systematic literature review as a methodology and address specific sectors, which fulfills particular research objectives but does not allow for an integrated view of cybersecurity and business.

Scientific databases have shown an uptick in publications on cybersecurity and business in recent years. However, this increase in published scientific articles is fragmented, and there is a need for more integration of this information (Aria & Cuccurullo, 2017). This lack of integration hampers the ability of researchers, managers, and policymakers to analyze the data effectively. For these reasons, scientific mapping is essential for scholars in all scientific disciplines as it allows for determining the intellectual structure and knowing the research front of scientific fields (Aria & Cuccurullo, 2017). Other researchers validate this methodology as the most appropriate for this type of study (Chaal *et al.*, 2023). Therefore, the primary motivation of the study lies in filling the knowledge gap and analyzing safety management, considering the interfaces between technology, people, and organizations through a bibliometric review of cybersecurity and business. Based on the arguments and problems identified, the authors will seek to answer the following research questions (RQ):

RQ_1. What is the cybersecurity and business knowledge base and its intellectual structure?

RQ_2. What is the cybersecurity and business research front?

As a methodology, the authors perform a bibliometric review through scientific mapping and performance analysis (Cobo *et al.*, 2011a). The research uses the Web of Science (WoS) database and Bibliometrix software (Aria & Cuccurullo, 2017) to analyze 410 articles and 1,355 authors on nine bibliometric indicators over 20 years. The research aims to assist academics, policymakers, and business decision-makers with cybersecurity management. This research is novel in proposing a bibliometric review of cybersecurity and business since the other studies addressed specific sectors and do not allow for an integrated vision of information on these two topics.

The main results reveal an upward publication trend with an annual growth of 27.63%. The United States of America (USA) has the highest scientific production, followed by the United Kingdom (UK) and China. As the main theoretical contribution, the study advances the frontier of knowledge by filling the identified knowledge gaps. On a practical level, the study can improve the analysis of academics, policymakers, and decision-makers in companies on safety management. The study presents future lines of research on cybersecurity and business, such as developing models and algorithms to reduce uncertainty. This manuscript is organized into seven parts. Section 2 presents the theoretical background. Section 3 explains the methodology. Section 4 presents the results. Section 5 details the discussion. Section 6 presents the limitations and future research. Section 7 indicates the study's conclusions, followed by the references used.

2. THEORETICAL BACKGROUND

A business is any organization involved in commercial, industrial, or professional activities, whether for profit or to fulfill a charitable or social mission (Hayes, 2020). This term also includes the efforts of individuals to produce and sell goods and services. Businesses can vary in size, and various fields of study are dedicated to understanding business administration (Hayes, 2020). Given the pressing and growing importance of cybersecurity and business concerns, it is imperative to conduct research in this field.

Cybersecurity is a crucial risk for any company due to the exponential increase in occurrences (Bresniker *et al.*, 2019) and sophistication of attacks (Abeshu & Chilamkurti, 2018). It refers to a set of methods, protocols, and tools to protect computer networks, software, data, and devices from unauthorized access, damage, or attacks (Boyson, 2014). Researchers warn of the emergence of organized, prepared, and persistent groups that attack companies for financial gain (Ahmad *et al.*, 2021). During the COVID-19 pandemic, cybercrime, such as fraud, increased above expected levels (Kemp *et al.*, 2021). These cyber-attacks lead to negative consequences for organizations, such as loss of productivity, lack of customer confidence, and legal penalties (Ahmad *et al.*, 2021). In addition, cyber risk can affect brand reputation, competitiveness, financial value, and business sustainability (Ngoc Thach *et al.*, 2021).

Other researchers advise that business and financial risk can impact the Sustainable Development Goals (SDGs) (Marti & Cervelló-Royo, 2023). In this direction, investment strategies for cybersecurity, disruptive technologies, and robotics can promote the SDGs without sacrificing business returns (Naffa & Fain, 2020). On the other hand, some authors point out that the increasing availability of the Internet has changed work and leisure activities by facilitating access to information and communication (Kemp *et al.*, 2021). However, criminals spend more time on online crimes, such as cyber fraud (Kemp *et al.*, 2021). Also, using the Internet in various sectors exposed companies more to cyber risks (Rashid *et al.*, 2021). For example, the number of cybercrime cases is steadily increasing in online e-banking (Ngoc Thach *et al.*, 2021). Healthcare organizations are also vulnerable to cyber threats, which can compromise data integrity and affect medical devices' functionality (Jalali *et al.*, 2019). Other researchers have identified that digital technology has transformed the healthcare sector by providing easy access to medical knowledge resources and improving clinical support and patient care. However, the use of technology in healthcare has raised concerns about privacy and security (Paul *et al.*, 2023). Table 1 presents an analytical summary of the leading publications.

Table 1
Analytical summary of the leading publications

Author(s)	Topic/Methods/Industry	Main contributions	Gaps/Suggestions for future research
Abeshu & Chilamkurti (2018)	Cyber-attacks/ Model development and comparison/ IoT and cloud computing	The study makes a notable contribution by introducing a deep learning method to enhance the detection of cyber-attacks within cloud-to-things computing. It tackles the shortcomings of conventional approaches and utilizes deep learning's strengths to bolster security in decentralized IoT settings.	Using deep learning in fog-to-things computing to detect distributed attacks demonstrates potential, yet notable gaps must be filled. Subsequent research should prioritize increasing model scalability, merging with edge computing, refining detection accuracy, and reducing false alarm rates to unlock deep learning's capabilities in this field fully.
Bresniker *et al.* (2019)	Threat detection/ Case study analysis/ Industry, academia, and government	The article urges a unified international initiative to utilize Artificial Intelligence (AI) and Machine Learning (ML) technologies in cybersecurity, highlighting their ability to revolutionize threat detection and response methods.	To maximize AI and ML's potential in cybersecurity, it is crucial to tackle collaboration, scalability, and data quality issues. Upcoming research should concentrate on building international partnerships, creating sophisticated threat detection models, and considering ethical aspects to establish strong and efficient cybersecurity solutions.
Jalali *et al.* (2019)	Healthcare cybersecurity/ Systematic Review/ Health Care	The document highlights a focus on technology-driven research in healthcare cybersecurity, noting significant gaps in nontechnological and physical security studies. It calls for more comprehensive investigations in these areas to enhance healthcare systems' overall security and safety.	The evaluation highlights the importance of expanding research efforts to incorporate non-technological elements and physical security within healthcare cybersecurity. Tackling these shortcomings can result in more robust and well-rounded cybersecurity approaches that improve the safety and dependability of healthcare delivery systems.
Naffa *et al.* (2020)	Cybersecurity/ Survey and data analysis/ Business context	The research indicates that investments focused on ESG megatrends can coincide with sustainability objectives without compromising financial returns, even though transaction expenses may affect net gains. This reinforces the potential of ESG investments to advance the SDGs while still achieving competitive performance.	Future studies should examine cost reduction's impact on long-term performance and incorporate recent data to identify trends. Addressing these gaps could enhance our understanding of the relationship between these investments, financial performance, and sustainability goals.
Bhamare *et al.* (2020)	Intrusion detection system/ Comprehensive Review/ Industrial	The article emphasizes improved cybersecurity for industrial control systems connecting with IT networks. It underscores the role of machine learning in developing strategies to safeguard industrial operations and critical infrastructures from emerging cyber threats.	The paper notes deficiencies in cybersecurity for Industrial Control Systems (ICS) in cloud environments and recommends future research on secure integration, advanced machine learning, and standardized security protocols.
Kemp *et al.* (2021)	Cybercrime/ Time-series analysis study/ Business context	The research emphasizes the necessity of flexible approaches to tackle cybercrime, particularly during major societal shifts such as the COVID-19 pandemic. It stresses the significance of recognizing the varied effects on different types of fraud and victim groups to address and reduce these crimes effectively.	Subsequent studies should focus on the diversity in victim experiences, investigate long-term effects, and conduct international comparisons to improve understanding and guide policy and practice.
Ahmad *et al.* (2021)	Situation awareness/ Case study analysis/ Business context	The research emphasizes how organizations can enhance situational awareness through management strategies. It highlights the need to understand the cyber-threat landscape and business context, which can significantly improve incident response.	Upcoming research should focus on filling these gaps by creating holistic models incorporating diverse viewpoints and improving communication and cooperation among different organizational areas.
NGOC Thach *et al.* (2021)	Cybersecurity risk management/ Case study analysis/ Banking	The study concludes that incorporating Industry 4.0 technologies in Vietnam's banking sector requires improved technology quality management and cybersecurity risks. The capacity to quickly respond to unexpected changes is vital for reducing cybersecurity threats and guaranteeing banking operations' secure and effective functioning.	The research highlights the significance of incorporating cutting-edge technologies in the banking sector while addressing cybersecurity threats. Nevertheless, more in-depth studies on risk evaluation, adaptation approaches, and the creation of customized cybersecurity frameworks are needed to assist the banking industry in Vietnam and comparable emerging economies more effectively.

Author(s)	Topic/Methods/Industry	Main contributions	Gaps/Suggestions for future research
Rashid *et al.* (2021)	Cybersecurity information sharing/ Model development and simulation analysis/ Business context	The document outlines an economic model that improves value creation and distribution in the cybersecurity information-sharing ecosystem. It highlights the critical role of end users in value generation and offers insights for business strategy and sustainability, particularly in cloud and edge computing.	The study highlights significant shortcomings in the sustainability of the cybersecurity information-sharing environment, especially within crowded markets, and emphasizes the importance of fair value allocation among all parties involved. Upcoming research should aim to create sustainable business models and investigate the incorporation of new technologies to improve the efficacy and robustness of the ecosystem.
Kappelman *et al.* (2022)	Cybersecurity/ Survey and data analysis/ Information technology	The research emphasizes a transition towards purposeful investments in IT and the increasing significance of cybersecurity and data analytics. It also points out the difficulties in recruiting qualified IT personnel and the changing responsibilities of CIOs in organizational leadership.	These studies indicate that upcoming research needs to tackle deficiencies in IT management areas, including Cybersecurity, Alignment, Analytics, Digital Transformation, and Compliance, as well as the difficulties in locating qualified experts in Cybersecurity, Analytics, AI, Functional Knowledge, and Cloud.
Manuel *et al.* (2022)	Cyber threats/ Model development and comparison/ Corporate and Public Sector	CyberTOMP plays a vital role in the industry by providing a practical, immediately applicable framework that improves the efficiency of cybersecurity management at both the tactical and operational tiers. It tackles the deficiencies found in existing high-level standards.	The CyberTOMP framework fills critical vulnerabilities in cybersecurity management by offering comprehensive procedural components for tactical and operational tiers. Subsequent studies aim to improve these methodologies, ensuring they are flexible and incorporated with overarching frameworks to efficiently handle cybersecurity in an ever-changing landscape.
Tagarev *et al.* (2022)	Cybersecurity networks/ Survey and data analysis/ Cybersecurity industry	The study emphasizes that strong governance and organizational frameworks are essential for effective collaborative cybersecurity networks. It identifies key business and governance models that can support these networks, particularly European Union initiatives.	The study points out gaps in skills and collaboration for effective cybersecurity networks. Future research should focus on governance structures and cross-industry collaboration to enhance cybersecurity efforts.
Kosmowski *et al.* (2022)	Cyber threats/ Integrated Evaluation Approach within a BCM/ Energy	The document presents a framework for integrating functional safety and cybersecurity assessments into business continuity management for energy companies using Industry 4.0 technologies. Focusing on prevention and recovery aims to mitigate cyber threat risks and enhance operational resilience.	Integrating functional safety and cybersecurity into a BCM framework is vital for protecting energy companies from cyber threats. Key gaps include better evaluation methods, standardization, and ongoing risk assessment. Future research should focus on developing integrated frameworks, secure communication protocols, real-time monitoring systems, and cross-industry collaboration.
Marti & Cervelló-Royo (2023)	Country risk/ Cluster analysis/ Countries	The paper presents a novel Sustainable Development Goal (SDG) achievement analysis based on the 2030 Agenda and its relationship with country risk, differentiating countries by income levels. The authors applied the Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS).	The study identifies limitations for future research, including the unclear relationship between country risk indicators and specific SDGs and data gaps in SDG scores that may overlook transboundary impacts. It stresses the importance of analyzing the evolution of SDGs and country risk indicators over time and updating indices to account for changes in country performance due to political leadership.
Paul *et al.* (2023)	Security and privacy issues/ Case study analysis/ Health Care	This article contributes by examining how digital technologies affect the healthcare sector and exploring the security and privacy issues related to digitalization in healthcare.	Future studies should focus on privacy and security regulations in healthcare, the impact of digitalization on patient outcomes, and the risks associated with wearable devices. Additional research opportunities include the role of artificial intelligence, the effects of blockchain technology, and patient involvement in privacy and security issues.

Author(s)	Topic/Methods/Industry	Main contributions	Gaps/Suggestions for future research
Javaheri *et al.* (2023)	Cyber-attacks/ Systematic survey/ Private companies, enterprises, and government agencies	The document discusses the complexities of cybersecurity, focusing on vulnerabilities to DDoS attacks that lead to financial and reputational harm. It reviews DDoS attacks and proposes a framework for understanding them, highlighting effective defense strategies such as fuzzy-based detection techniques to improve intrusion detection systems.	The paper emphasizes challenges in fuzzy anomaly detection due to large datasets and high dimensionality, calling for more research in feature selection, online training, and incremental learning for DDoS detection. It also highlights the need for standardized, updated datasets with real network traces to evaluate emerging security attacks better.
Corallo *et al.* (2023)	Cybersecurity issues in Industry 4.0/ Single case study with multiple units of analysis/ Aeronautical	The document evaluates cybersecurity issues in Industry 4.0, providing insights for researchers and businesses. By using impact assessment methodology, companies can improve the security of critical manufacturing data and mitigate cyber-attack risks in innovative manufacturing environments.	The document highlights cybersecurity challenges in manufacturing systems 4.0, especially in the aeronautical sector, and suggests that broader research across various sectors and strategies could improve threat management in advanced manufacturing.

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

Risks arise when companies adopt Industry 4.0 technologies in the industrial sector (Kosmowski *et al.*, 2022), as computer systems remain highly vulnerable to various types of distributed denial of service (DDoS) attacks (Javaheri *et al.*, 2023). The lack of adequate security in new multi-cloud platforms can cause high costs associated with security breaches in real-time industrial platforms (Bhamare *et al.*, 2020) and introduce new challenges in cybersecurity, such as identifying critical assets to protect against cyberattacks and evaluating commercial impacts (Corallo *et al.*, 2023). Cloud computing for Industrial Control Systems (ICS), present in industrial sectors and critical infrastructures, shows advantages such as scalability, cost-effectiveness, and flexibility (Bhamare *et al.*, 2020). However, by moving to the cloud, ICSs may become exposed to new threats and vulnerabilities (Bhamare *et al.*, 2020). Other researchers associated potential security issues with using open systems and networks for communication and control (Kosmowski *et al.*, 2022). To address these drawbacks and achieve an adequate level of cybersecurity, technological solutions, such as antivirus software, firewalls, intrusion detection systems, virtual private networks, access control systems, and content filters, need more advanced and collaborative approaches (Rashid *et al.*, 2021).

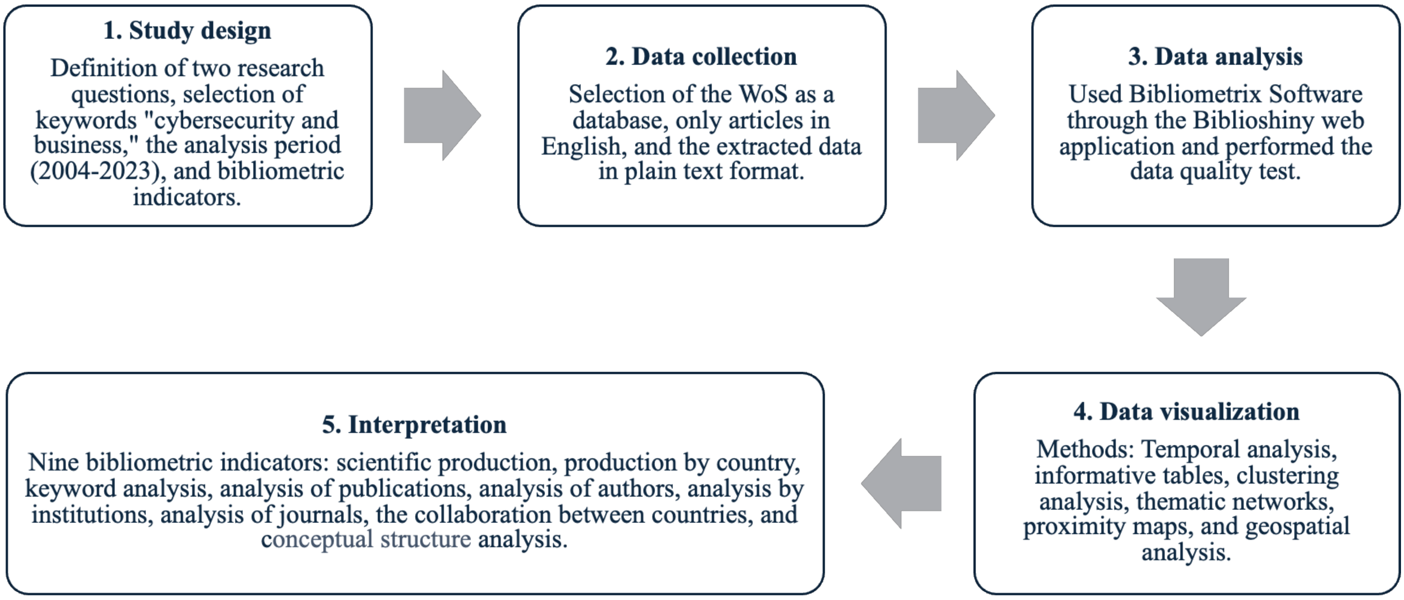
Moreover, critical infrastructures such as nuclear and thermal power plants, water treatment facilities, heavy industries, and distribution systems may expose new threats and vulnerabilities (Bhamare *et al.*, 2020). Cyber-attack problems may also disrupt the energy sector, such as industrial energy companies, power plants, and distributed renewable energy plants (Kosmowski *et al.*, 2022). For these reasons, cybersecurity is a growing concern for most organizations (Kappelman *et al.*, 2022).

A lack of investment in cybersecurity impacts increased risks, economic costs of incidents, societal losses, and reduced levels of individual and national security (Rashid *et al.*, 2021). Therefore, organizations need to invest in cybersecurity to adapt quickly and effectively and improve the quality of technology management (Ngoc Thach *et al.*, 2021). In this direction, information technology (IT) spending levels return from Covid-induced peaks in 2020 (Kappelman *et al.*, 2022). Managers also need to understand how organizations can protect against sophisticated and persistent cyberattacks; this is a significant challenge for research and practice (Ahmad *et al.*, 2021). In addition, the industrial sector needs to understand the risks posed by potential cyberattacks when adopting Industry 4.0 technologies (Kosmowski *et al.*, 2022). However, the different cybersecurity reference models are not directly applicable to lower levels due to the lack of specific procedural details. Therefore, organizations need a methodological basis to manage cybersecurity at these levels (Manuel *et al.*, 2022). For other researchers, an effective response to advanced cyber threats requires investment in greater awareness, trained personnel, and cutting-edge technology (Tagarev *et al.*, 2022). However, only a few companies have the resources to offer comprehensive solutions and maintain high technological expertise. The same study highlights a possible solution for creating a network of cybersecurity competence centers (Tagarev *et al.*, 2022).

In summary, the articles analyzed reveal the importance of understanding and protecting against cyberattacks, the challenges in applying reference models in cybersecurity, and the need for a methodological basis for organizations.

3. METHODOLOGY

Bibliometrics involves using quantitative methods to study bibliographic material in library and information sciences (Pritchard, 1969; Broadus, 1987). Eugene Garfield created this research discipline in 1955 (Garfield, 1955), and it is a widely used approach to summarizing key findings from a collection of bibliographic documents (Martínez-López *et al.*, 2018). The bibliometric review follows a combined approach (Noyons *et al.*, 1999) with scientific mapping and performance analysis in this research. Scientific mapping seeks to construct bibliometric visualizations showcasing the conceptual, intellectual, and social structure of specific disciplines, scientific domains, or research fields (Cobo *et al.*, 2011b). On the other hand, performance analysis shows the evaluation of groups of scientists and the impact of their activity on the bibliographic database (Cobo *et al.*, 2011a). The authors use a five-stage structured workflow to perform the bibliometric review (Zupic & Čater, 2015). Figure 1 presents the workflow applied in this paper.



1. Study design
Definition of two research questions, selection of keywords "cybersecurity and business," the analysis period (2004-2023), and bibliometric indicators.

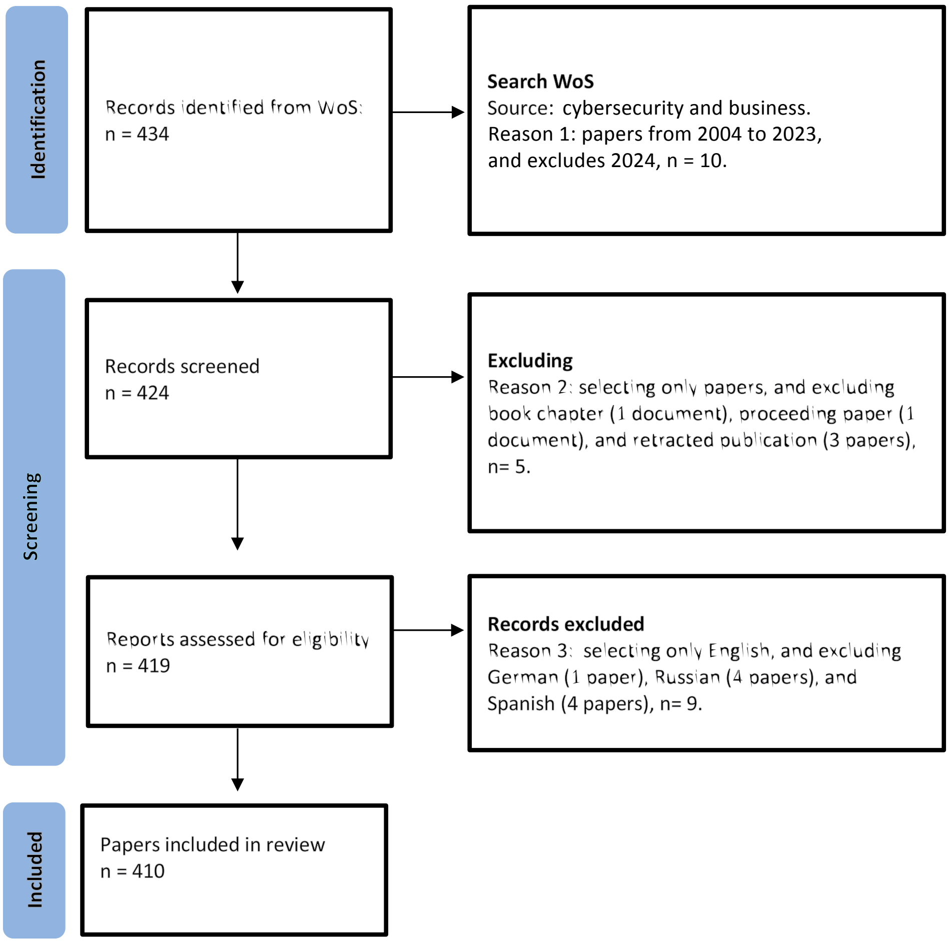
2. Data collection
Selection of the WoS as a database, only articles in English, and the extracted data in plain text format.

3. Data analysis
Used Bibliometrix Software through the Biblioshiny web application and performed the data quality test.

4. Data visualization
Methods: Temporal analysis, informative tables, clustering analysis, thematic networks, proximity maps, and geospatial analysis.

5. Interpretation
Nine bibliometric indicators: scientific production, production by country, keyword analysis, analysis of publications, analysis of authors, analysis by institutions, analysis of journals, the collaboration between countries, and conceptual structure analysis.

Figure 1
Methodology workflow applied in this paper
Source: Own elaboration based on Zupic and Čater (2015).



Records identified from WoS:
n = 434

Search WoS
Source: cybersecurity and business.
Reason 1: papers from 2004 to 2023, and excludes 2024, n = 10.

Records screened
n = 424

Excluding
Reason 2: selecting only papers, and excluding book chapter (1 document), proceeding paper (1 document), and retracted publication (3 papers), n= 5.

Reports assessed for eligibility
n = 419

Records excluded
Reason 3: selecting only English, and excluding German (1 paper), Russian (4 papers), and Spanish (4 papers), n= 9.

Papers included in review
n = 410

Figure 2
The PRISMA flowchart via WoS
Source: Own elaboration based on Page *et al.* (2021).

The first stage consists of the study's design, which includes the research questions presented in the introduction, the selection of keywords, the definition of the period of analysis and the bibliometric indicators (Pedraja-Rejas *et al.*, 2022). The selection of keywords helps to determine the study sample (Blanco-Mesa *et al.*, 2019), and the authors searched with 14 words organized into two sets of topics. The first set includes cybersecurity, cyber security, cyber-attacks, cyber risks, cyber fraud, cybercrime, and cyber threats. The second set covers business, enterprise, entrepreneurship, organizations, firms, industry, and business sustainability. As a result, the authors verified that the keywords in the topic section are "cybersecurity" AND "business" and represent the central themes of the research. The authors conducted a longitudinal study between 2004 and 2023, covering 20 years. Before this period, no articles were published with the keywords "cybersecurity" AND "business". The authors then choose nine indicators: scientific production, production by country, keyword analysis, publication analysis, author analysis, institution analysis, journal analysis, cross-country collaboration, and conceptual structure analysis. Bibliometric indicators can assist in understanding the caliber of academic work being assessed and in making an assessment, thus serving as a tool for evaluating research (Moed, 2005).

The second stage is for data collection, and the authors select the Web of Science (WoS) database. For some researchers WoS is preferable to other databases regarding data quality. For example, the reference elements in Scopus must be standardized and combined. On the other hand, in Dimensions, the algorithm that classifies the search areas could be more efficient (Aria & Cuccurullo, 2017). The authors use the keywords "cybersecurity" and "business" from 2004 to 2023 and excludes 2024. This gives a total of 424 papers. A filter is applied to focus specifically on research contributions by selecting only papers and excluding book chapters, proceeding papers, and retracted publications. This refines the results to 419 papers. An additional filter is applied for languages by selecting only English and excluding German, Russian, and Spanish. This refines the results to 410 papers, which will be used to create tables and figures with WoS. It is worth noting that the Prisma flowchart in Figure 2 can also be generated with WoS.

Data were extracted from WoS from May 1st, 2024, in plain text format. This format is preferable to others, as the BibTeX format of Scopus and the CSV format of Dimensions do not allow exporting some metadata (Aria & Cuccurullo, 2017). Table 2 provides a comprehensive overview of our meticulous data collection process. The key findings reveal 410 articles, demonstrating a robust 27.63% annual growth rate. We also identified 1,540 author keywords, 1,355 authors, and a 31.46% international co-authorship. These findings underscore the academic interest in this topic and highlight this research's global reach and collaborative nature.

The third stage is devoted to data analysis, and the authors employ the Bibliometrix software through the Biblioshiny web application to analyze the articles. The authors preferred this software tool, as other specialized tools usually perform only some steps of the scientific mapping analysis (Aria & Cuccurullo, 2017). Researchers used Bibliometrix and Biblioshiny to identify the most impactful studies on customer churn and map their field's conceptual and intellectual structure (Ribeiro *et al.*, 2022). Other researchers used this software to understand the impact of the informal economy and digital platforms (Silva & Moreira, 2022). This open-source tool allows a complete analysis of scientific literature mapping. In addition, it is a friendly tool for non-programmers, facilitating the application of this type of study by other scholars in their field of research.

After finishing the database loading, the authors performed a data quality test in Bibliometrix. The results showed that the metadata does not present critical problems, and most indicators are at excellent and good levels. Thus, the authors proceed with the data analysis.

Table 2
Data collection results

Description	**Results**
MAIN INFORMATION ABOUT DATA	
Timespan	2004:2023
Sources (Journals, Books, etc.)	251
Documents	410
Annual Growth Rate %	27.63
Document Average Age	3.1
Average citations per doc	12.64
References	21231
DOCUMENT CONTENTS	
Keywords Plus (ID)	564
Author's Keywords (DE)	1540
AUTHORS	
Authors	1355
Authors of single-authored docs	62
AUTHORS COLLABORATION	
Single-authored docs	66
Co-Authors per Doc	3.54
International co-authorships %	31.46
DOCUMENT TYPES	
article	410

Note: DE (the frequency distribution of authors' keywords); ID (the frequency distribution of keywords associated to the manuscript by Thomson Reuters' ISI Web of Knowledge database).

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

The fourth stage of our study is dedicated to data visualization, a crucial step in presenting our findings clearly and meaningfully. Bibliometric networks can be visualized or modelled graphically (Aria & Cuccurullo, 2017). The networkPlot function, which can display a network generated by biblioNetwork using R routines or VOS viewer software (van Eck & Waltman, 2010), is particularly useful in this context. The authors employed diverse methods, including temporal analysis, informative tables, clustering analysis, thematic networks, proximity maps, and geospatial analysis (Aria & Cuccurullo, 2017). Each technique was carefully chosen to represent the data best and enhance understanding. The final stage involves data interpretation, where we delve deeper into the results of our bibliometric review, offering valuable insights and implications.

4. RESULTS OF THE BIBLIOMETRIC REVIEW

4.1. Scientific production

Scientific production is a crucial indicator of research output, reflecting academics' efforts to push the boundaries of knowledge and address societal needs (Barcellos-Paula *et al.*, 2022). Table 2 reveals that scientific production is concentrated in the last five years (2019-2013), representing 90.45% of the 859 publications. This result indicates the novelty of the topic and its emerging significance, as it is being investigated more strongly in the countries, reinforcing this study's importance. Also, the results show that this topic is relevant to academia, and studies in this field are expanding due to the advancement of technology in business sectors (Paul *et al.*, 2023).

4.2. Production by countries

This indicator reveals that the USA leads this ranking with 270 publications, followed by the UK with 98 publications and China with 52. Table 3 reflects the current state of research in the intersection of cybersecurity and business, with the USA maintaining a significant lead, the UK showing steady growth, and China emerging as a strong contender.

Other relevant data shows that the USA was the pioneer country, with the first publication on cybersecurity and business in 2004. Between 2009 and 2013, there were seven publications, increasing to 39 publications from 2014 to 2018. Finally, in 2019-2023, 223 publications were registered from USA, further underlining the growing importance of this research area.

Table 3
Top 20 - Production by countries

Countries	D1	D2	D3	D4	TP
USA	1	7	39	223	270
UK	0	0	11	87	98
China	0	0	1	51	52
Australia	0	0	8	40	48
Saudi Arabia	0	0	0	41	41
Italy	0	0	8	32	40
Spain	0	0	2	37	39
Ukraine	0	0	0	33	33
India	0	0	0	28	28
Malaysia	0	0	1	27	28
South Korea	0	0	1	24	25
Germany	0	0	0	22	22
Poland	0	0	0	22	22
Canada	0	0	2	18	20
Pakistan	0	0	0	19	19
Russia	0	0	0	19	19
Greece	0	0	0	18	18
Netherlands	0	0	0	13	13
Sweden	0	0	0	13	13
France	0	0	1	10	11
Total	1	7	74	777	859
%	0.12%	0.81%	8.61%	90.45%	100%

Abbreviations: D1=2004-2008; D2=2009-2013; D3=2014-2018; D4=2019-2023; TP = total publications; % = percentage of publications.

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

4.3. Keywords analysis

This indicator has a simple word count based on the keywords plus (Aria & Cuccurullo, 2017). The research uses the word cloud method to analyze keywords, with the word size representing the number of occurrences. Figure 3 shows that the most frequent words are security, internet, and impact.

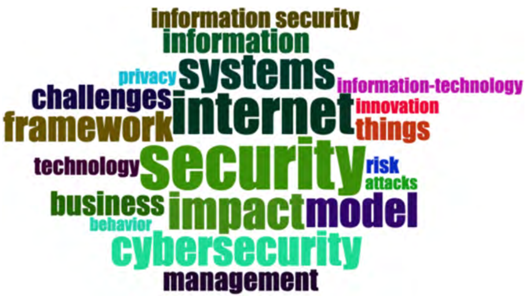


Figure 3
Word cloud "cybersecurity" and "business"

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

Table 4
Top 20 - Most frequent words

Words	D1	D2	D3	D4	TO
security	0	0	3	32	35
internet	0	0	1	28	29
impact	0	0	0	25	25
systems	0	0	0	24	24
cybersecurity	0	1	1	21	23
model	0	0	2	21	23
framework	0	0	4	16	20
business	0	0	0	16	16
challenges	0	0	0	16	16
information	0	0	0	16	16
management	0	0	1	14	15
things	0	0	1	14	15
information security	0	0	2	11	13
technology	0	0	0	12	12
risk	0	0	0	11	11
information-technology	0	0	0	10	10
innovation	0	0	0	10	10
privacy	0	0	0	10	10
attacks	0	0	2	7	9
behavior	0	0	0	9	9
Total	0	1	17	323	341
%	0%	0.29%	4.99%	94.72%	100%

Abbreviations: D1=2004-2008; D2=2009-2013; D3=2014-2018; D4=2019-2023; TO = total occurrences. % = percentage of occurrences.

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

Table 4 presents a list of the 20 most frequent words. The results reveals that 94.72% of the words have occurred in the last five years (2019-2023) and shows that the first position is security, with 35 occurrences; internet, with 29; and impact, with 25. This outcome reinforces that the word "security" is more consolidated and present in most publications. On the other hand, business is in eighth position among the most used words, indicating a research opportunity in this study area. In 2023, the trending topics were information, innovation, and trust, reflecting the evolving research landscape at the intersection of cybersecurity and business.

4.4. *Analysis of publications*

This subsection analyzes the most cited papers by considering the number of times each manuscript has been cited (TC), the average annual number of times each manuscript has been cited (TC per year), and the overall normalized citation count (normalized TC). The normalized TC is calculated by dividing the actual count of cited items by the expected citation index for papers with the same year of publication (Aria & Cuccurullo, 2017). Table 5 presents a list of the 20 most cited papers. The results indicate that the first place goes to Babiceanu and Seker (2016) with 285 citations, followed by Nishant *et al.* (2020) with 207 citations, and in third place Abeshu and Chilamkurti (2018), with 185 citations. The main articles are listed below.

Table 5
Most globally cited documents

Author-year	Journal	TC	TCY	NTC
(Babiceanu & Seker, 2016)	Comput Ind	285	31.67	5.09
(Nishant *et al.*, 2020)	Int J Inform Manage	207	41.40	10.90
(Abeshu & Chilamkurti, 2018)	IEEE Commun Mag	185	26.43	4.75
(Al-rimy *et al.*, 2018)	Comput Secur	169	24.14	4.34
(Knowles *et al.*, 2015)	Int J Crit Infr Prot	160	16.00	2.86
(Ghobakhloo, 2020)	Int J Prod Res	123	24.60	6.48
(Shah, 2020)	Pain Physician	119	23.80	6.27
(Leng *et al.*, 2021)	IEEE T Syst Man Cy-S	114	28.50	8.83
(Li *et al.*, 2019)	Int J Inform Manage	111	18.50	6.31
(Corallo *et al.*, 2020)	Comput Ind	107	21.40	5.64
(Bhamare *et al.*, 2020)	Comput Secur	101	20.20	5.32
(Hasanova *et al.*, 2019)	Int J Netw Manag	73	12.17	4.15
(Gupta *et al.*, 2020)	Int J Inform Manage	66	13.20	3.48
(Boyson, 2014)	Technovation	60	5.45	1.88
(Kure *et al.*, 2018)	Appl Sci-Basel	59	8.43	1.51
(Asghar *et al.*, 2019)	Comput Netw	51	8.50	2.90
(Protogerou *et al.*, 2021)	Evol Syst-Ger	46	11.50	3.56
(Kappelman, Johnson, *et al.*, 2018)	Mis Q Exec	44	6.29	1.13
(Kemp *et al.*, 2021)	J Contemp Crim Just	42	10.50	3.25
(Mendhurwar & Mishra, 2021)	Enterp Inf Syst-Uk	41	10.25	3.18

Abbreviations: TC = total citations; TCY = total citations per year; NTC = normalized total citations.

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

Babiceanu and Seker (2016) analyze the landscape and prospects of big data and virtualization manufacturing cyber-physical systems (CPS). They highlight the ability of these technologies to transform manufacturing operations by providing better connectivity, forecasting capabilities, and more effective decision-making while highlighting the urgent need for robust cybersecurity protocols. Nishant *et al.* (2020) examine how AI can aid sustainability, emphasizing its ability to bring about significant change and the obstacles that must be overcome. It establishes a research framework that promotes a comprehensive method, incorporating multiple fields to guarantee AI's responsible and sustainable use.

4.5. *Analysis of authors*

This indicator calculates and plots the production of the most relevant authors (number of publications and total citations per year) over time. Figure 4 shows the results. Kappelman, Maurer, and Torres lead with six publications.

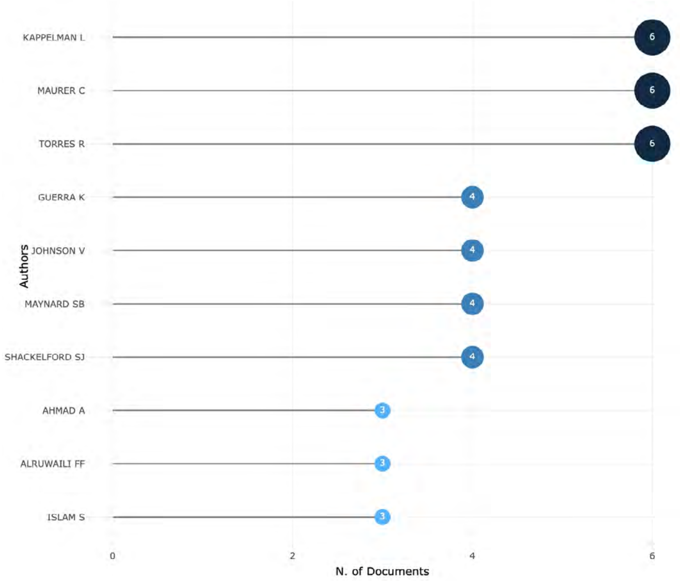


Figure 4
Most relevant authors

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

Table 6 shows the production of the most relevant authors, including the year of publication, number of citations, and total citations per year. The most cited documents are Kappelman, Johnson, *et al.* (2018), Kappelman *et al.* (2019) and Kappelman, Torres, *et al.* (2018).

Table 6
Most relevant authors

Author-year	Document	TC	TCY
Kappelman *et al.* (2018)	The 2017 SIM IT issues and trends study	44	6.286
Kappelman *et al.* (2019)	A study of information systems issues, practices, and leadership in Europe	33	5.500
Kappelman *et al.* (2018)	The 2018 SIM IT issues and trends study	32	5.333
Kappelman *et al.* (2021)	The 2020 SIM IT issues and trends study	13	3.250
V. Johnson *et al.* (2023)	The 2022 SIM IT issues and trends study	3	1.500
Kappelman *et al.* (2022)	The 2021 SIM IT issues and trends study	3	1.000
Klaus *et al.* (2022)	Prioritizing IT management issues and business performance	1	0.333

Abbreviations: TC = total citations; TCY = total citations per year.

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

Kappelman, Johnson, *et al.* (2018) state that in 2017, the primary recent IT expenditure was in Business Analytics, with Security, Cloud, Software Development, and ERP following closely behind. The most concerning IT management challenges for CIOs (Chief information officer) include Cybersecurity, IT Talent Shortage, alignment between business and IT, and Compliance and Regulation. IT executives' top concerns 2017 were alignment, digital transformation, cybersecurity, costs, and business agility (Kappelman, Johnson, *et al.*, 2018). The primary IT investments in 2018 were analytics, cybersecurity, cloud, software development and maintenance, and ERP (Kappelman, Torres, *et al.*, 2018). IT spending as a percentage of revenue has slightly increased, but it has remained similar to the 10-year average of 5.7%. The top concerns for IT management in 2022 are Cybersecurity, Alignment, Analytics, Compliance, and Digital Transformation. Significant IT investments include analytics, cybersecurity, cloud, application development, and enterprise resource planning (ERP) (Johnson *et al.*, 2023). Researchers found that companies prioritizing cybersecurity/privacy and IT-business alignment exhibit greater profitability than those not (Klaus *et al.*, 2022).

4.6. *Analysis by institutions*

The institutions are ranked based on scientific production and collaborative networks. Figure 5 shows Indiana University System is in first place with 19 publications, Indiana University Bloomington in second place with 18, and the State University System of Florida in third place with 15.

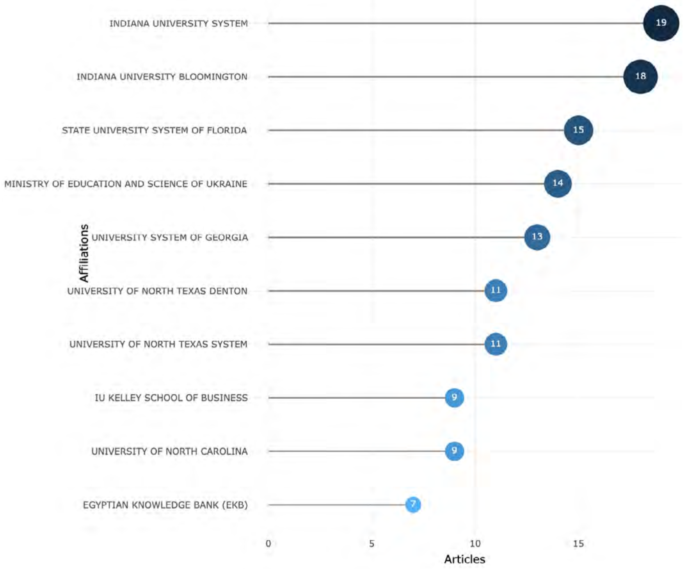


Figure 5
Most relevant affiliations

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

Figure 6 presents a temporal analysis of the scientific production of the affiliations. In 2023, Indiana University System solidified its position as the leading institution in the intersection of cybersecurity and business. All affiliations grew in publication numbers, reflecting a competitive landscape and diverse research contributors.

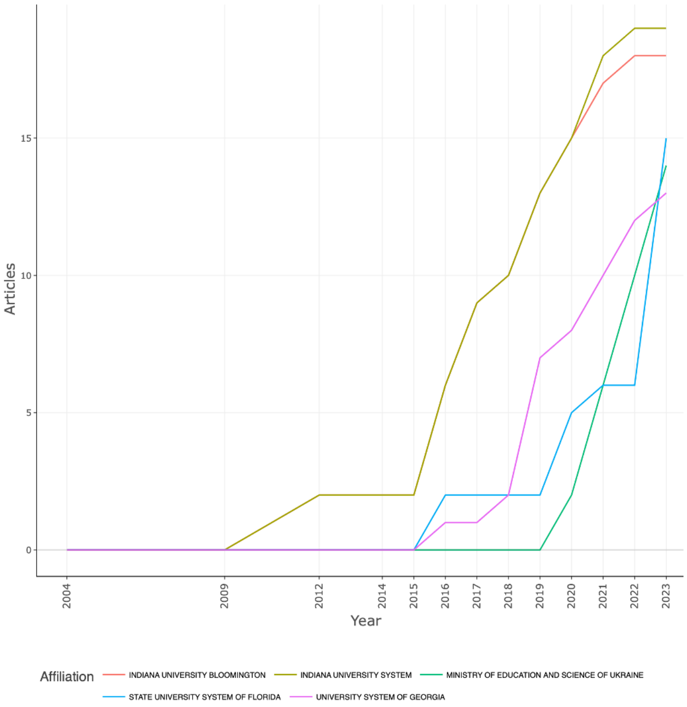


Figure 6
Scientific production of affiliations over time

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

4.7. *Analysis of journals*

This indicator is relevant as scientific journals are essential in disseminating knowledge (Barcellos-Paula *et al.*, 2022). Figure 7 shows an analysis of the most influential journals. Business Horizons and IEEE Access are tied for first place with 17 publications each, followed by Computers & Security with 15.

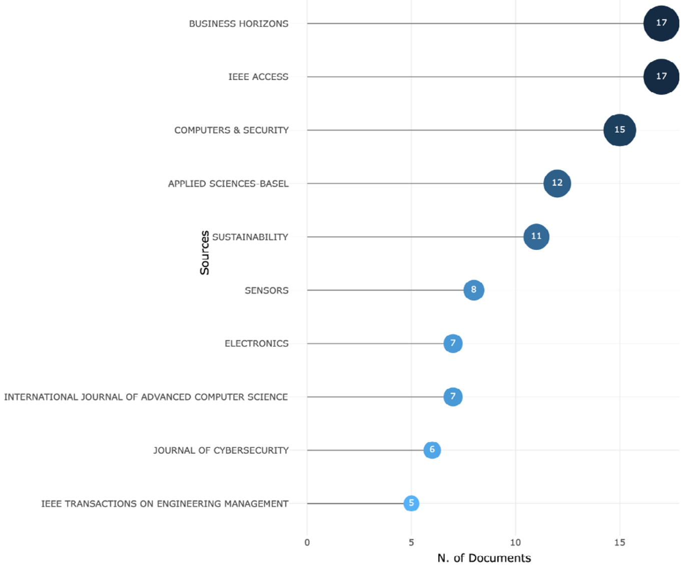


Figure 7
Most influential journals

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

4.8. *Collaboration between countries*

This indicator shows links between international scientific cooperation and knowledge dissemination globally. Figure 8 indicates that the USA leads worldwide collaborations with Australia, Canada, China, Saudi Arabia, and India. Notable collaborations include the UK, Spain, China, and Korea.

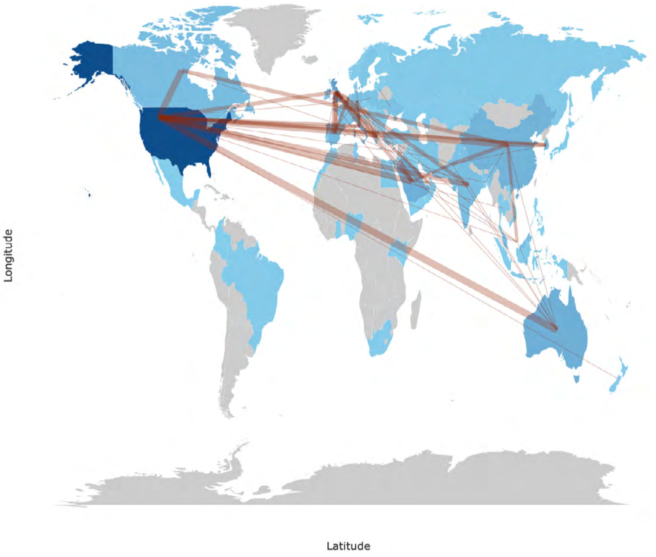


Figure 8
Collaboration between countries
Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

4.9. *Conceptual Structure Analysis*

This subsection discusses two types of analysis based on conceptual structure. The first type uses a network approach with stages including thematic evolution, thematic map, and co-occurrence networks. The second type uses a factorial approach involving a map of words and a dendrogram of words.

4.9.1. Network Approach

Thematic evolution analysis

The first stage addresses the thematic evolution analysis based on co-word network analysis and clustering (Cobo *et al.*, 2011a). The thematic evolution is divided into more relevant periods between the research topics: 2004-2014, 2015-2018, and 2019-2023. Figure 9 display the thematic evolution.

Research from 2004-2014 focused on cybersecurity, including viewing information risk as a challenge and integrating risk analysis into business decisions (Johnson *et al.*, 2009). There was also research on “Supply Chain Cyber Risk Management”, which merges cybersecurity, supply chain management, and enterprise risk management (Boyson, 2014).

During the second period (2015-2018), research focused on cybersecurity, risk management, cyberattacks, and cloud computing. For instance, Knowles *et al.* (2015) provide valuable insights by reviewing existing approaches to cybersecurity management in industrial control systems, pinpointing crucial deficiencies in security metrics, and suggesting avenues for future research. Additionally, it presents the idea of functional assurance to strengthen the resilience and security of industrial control systems. Babiceanu and Seker (2016) proposed a framework for designing predictive cyber-physical systems integrated with IoT and big data analytics to improve manufacturing operations and control. Another research presented a decision model for companies to evaluate investing in on-premises IT infrastructure instead of outsourcing IT services in a multi-cloud environment, aiming to reduce costs and security risks (Hosseini-Shirvani *et al.*, 2018).

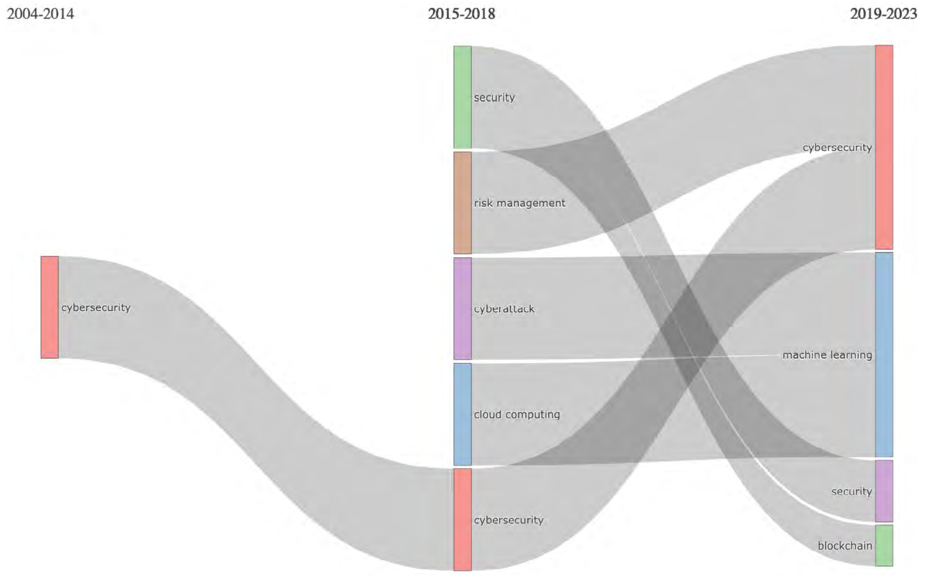


Figure 9
Thematic evolution
Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

The third period (2019-2023) focused on cybersecurity, machine learning, security, and blockchain. Hasanova *et al.* (2019) researched blockchain cybersecurity vulnerabilities and suggests countermeasures. Blockchain technology has broad applications beyond cryptocurrencies, using peer-to-peer networks and distributed systems to store transactions in linked blocks. Despite being considered secure, it has faced successful cyber-attacks (Hasanova *et al.*, 2019). Nishant *et al.* (2020) suggested that AI can revolutionize companies and address sustainability issues. Organizations can reduce natural resources and energy intensity, but challenges include over-reliance on historical data and uncertain human behavior. Future research must consider multiple factors to demonstrate immediate AI solutions without compromising environmental sustainability (Nishant *et al.*, 2020). In 2022, a study highlighted security vulnerabilities in IoT environments. The researchers proposed a multi-level DDoS mitigation approach using a device-based blockchain verification mechanism developed using Hyperledger Caliper (Hayat *et al.*, 2022). Finally, the research conducted by Corallo *et al.* (2023) demonstrates that the impact assessment methodology can assist companies in recognizing essential assets and evaluating the business implications of cybersecurity incidents in manufacturing systems 4.0.

Thematic map analysis

In the second stage, the thematic map analysis includes co-word analysis to extract clusters of keywords. The strategic diagram identifies four different types of topics based on their position in a quadrant: Motor themes (A), Basic topics (B), Peripheral topics (C), and Niche topics (D) (Aria & Cuccurullo, 2017). Figure 10 shows the results with nine clusters.

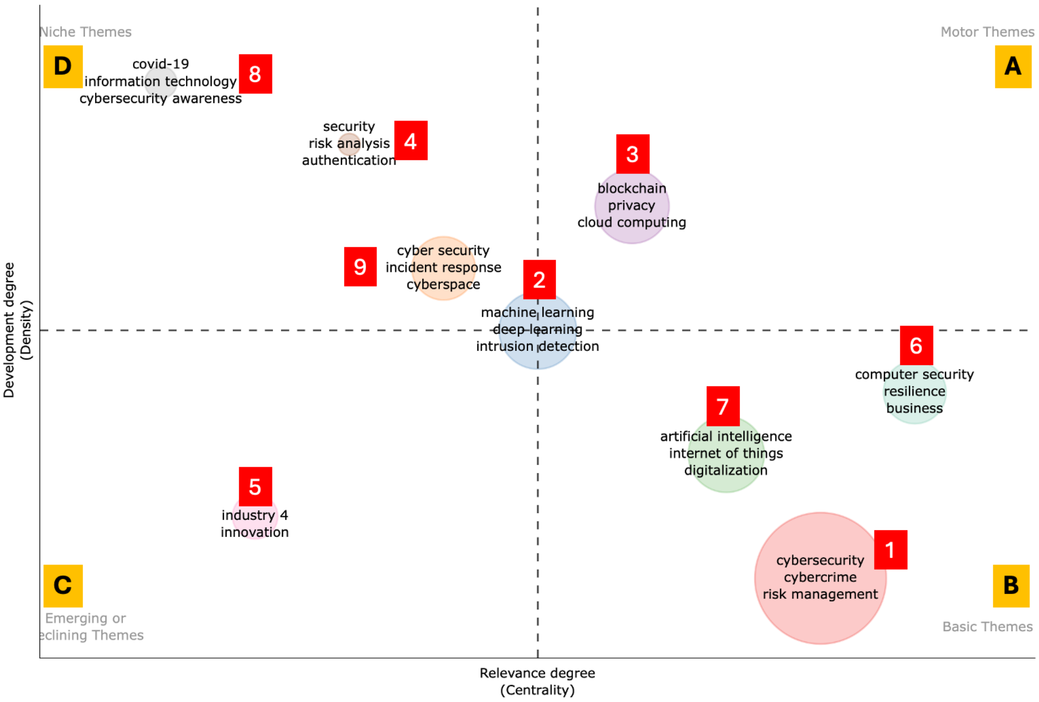


Figure 10
Thematic map
Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

In quadrant A, cluster 3 stands out, consisting of the driving topics of blockchain, privacy, and cloud computing. This result indicates that cluster 3 represents well-developed and meaningful concepts that form the domain's core framework. It is worth highlighting cluster 2, which consists of machine learning, deep learning, and intrusion detection, in the center of the diagram.

In quadrant B, cluster 1 stands out, consisting of cybersecurity, cybercrime, and risk management. We have highlighted some influential investigations in cybersecurity. The first research uses Cyber Threat Intelligence (CTI) and Machine Learning (ML) to predict cyber threats and improve supply chain security (Yeboah-Ofori *et al.*, 2021). The second paper examines the impact of cyber-attacks on companies and the role of cyber risk insurance (Shackelford, 2012). The third study introduces a decision-support framework for optimal cybersecurity investment (Tsiodra *et al.*, 2023). The fourth investigation provides a detailed analysis of a prominent financial institution with a well-established incident response capability developed from prior attack incidents (Ahmad *et al.*, 2021). The last paper discusses using blockchain technology for secure and transparent digital forensic investigations (Khan *et al.*, 2021). Cluster 7 stands out: artificial intelligence, the Internet of Things, and digitalization. Cluster 6 is also observed, consisting of computer security, resilience, and business. These results indicate that these topics are significant across different areas of the domain. On the other hand, in quadrant D, cluster 9 (cyber security, incident response, and cyberspace), cluster 4 (security, risk analysis, and authentication), and cluster 8 (COVID-19, information technology, and cybersecurity awareness) stand out as niche topics, suggesting that they are strongly developed yet marginal within the studied domain. Finally, in quadrant C, cluster 5 stands out as an emerging or declining topic, consisting of industry 4.0 and innovation, indicating that they are not fully developed or only marginally relevant.

Co-occurrence network analysis

In the third stage, network analysis shows the connections between the author's keywords. This helps visualize links between words and identify different groupings. Each color represents a grouping, the node size represents occurrence, and the line thickness shows co-occurrence. Figure 11 displays co-occurrences.

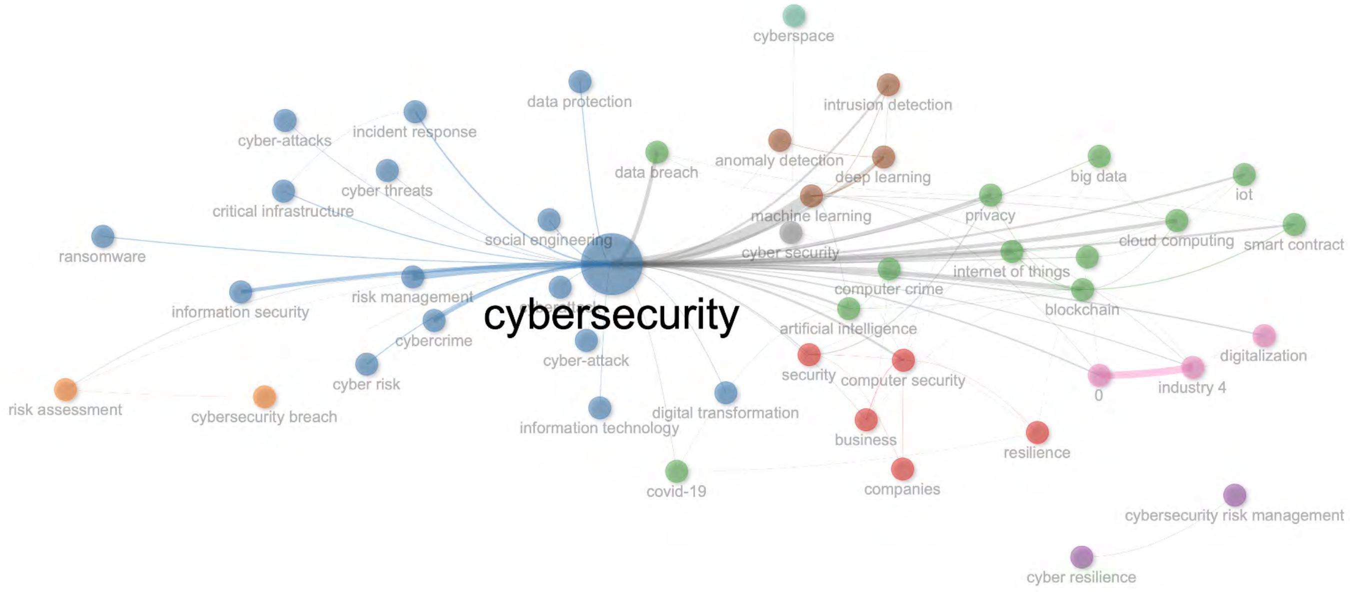


Figure 11

The co-occurrences between cybersecurity and business

Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

The results show nine clusters. The cybersecurity cluster (blue) has 16 interconnected words, such as risk management and cybercrime. For instance, research seeks solutions to combat the increase in cyber-attacks in various parts of the world (Bresniker *et al.*, 2019), propose effective defensive strategies (Javaheri *et al.*, 2023), reduce uncertainty in the management process (Kosmowski *et al.*, 2022), and help improve business sustainability (Javaheri *et al.*, 2023).

The artificial intelligence cluster (green) has 12 interconnected words, including blockchain and the Internet of Things. The security cluster (red) has five interconnected words, such as computer security and business. This helps visualize the terms associated with cybersecurity and business, confirming the research's relevance.

4.9.2. Factorial analysis

Factorial analysis is a technique that helps understand the underlying structure of a framework by analyzing word associations within a network. It uses the R package Bibliometrix, which employs Multiple Correspondence Analysis (MCA) through the author's keywords to identify shared concepts and K-means clustering to group-related documents. MCA produces a concise representation of the original data by performing a homogeneity analysis of a matrix of indicators (Aria & Cuccurullo, 2017). The first outcomes of the factorial analysis are depicted in Figure 12.

The results are interpreted based on the relative positions of the points and their distribution along the four dimensions. Dimension 1 covers cybersecurity, cybercrime, risk management, and information security. For instance, as for Abeshu and Chilamkurti (2018), they reveal that traditional cryptographic solutions and machine learning-based attack detection mechanisms have limitations for IoT. For these reasons, they propose a distributed deep learning scheme to detect cyber-attacks in fog computing with higher accuracy, lower false alarm rates, and higher scalability than shallow models.

Dimension 2 encompasses machine learning, the Internet of Things, cloud computing, artificial intelligence, and blockchain. For example, Babiceanu and Seker (2016) review virtualization and cloud-based services for manufacturing systems and propose a framework for predictive manufacturing cyber-physical systems with Internet of Things and Big Data analytics capabilities. Nishant *et al.* (2020) highlight the potential of Artificial Intelligence (AI) to promote environmental governance. While AI can help reduce the use of natural resources, research on AI for sustainability faces challenges such as reliance on historical data, uncertain human behavior, cybersecurity risks, negative impacts, and measurement challenges.

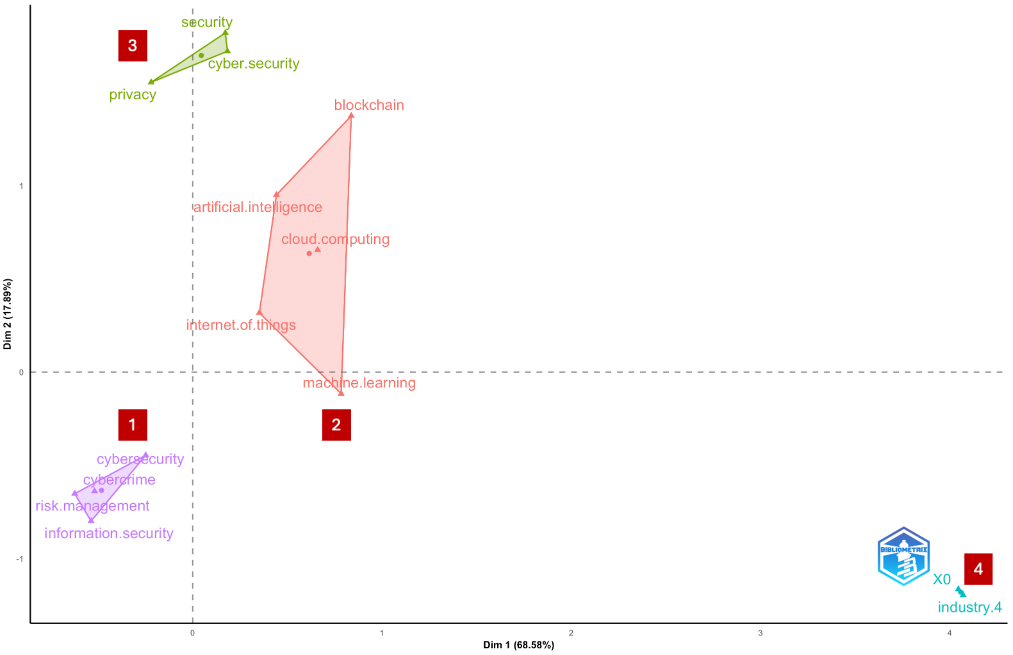


Figure 12
Conceptual structure map-method: MCA
Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

Dimension 3 contains security, cyber security, and privacy. In addition, dimension 4 includes Industry 4.0. For instance, Leng *et al.* (2021) contribute to understanding blockchain's role in enhancing smart manufacturing by identifying key cybersecurity challenges and proposing metrics for effective implementation. It also sets a foundation for future research to address these challenges, promoting the secure and intelligent evolution of Industry 4.0. It should be noted that the map's origin represents the average position of all column profiles, and therefore, dimension 1 represents the center of the research field, confirming that cybersecurity and risk management are the most common and significant shared themes.

Additionally, Bibliometrix allows a correspondence and grouping analysis to be carried out through a dendrogram of words. This helps to understand the relationship between the topics and corroborates the findings of the conceptual structure map-method. Figure 13 shows the results.

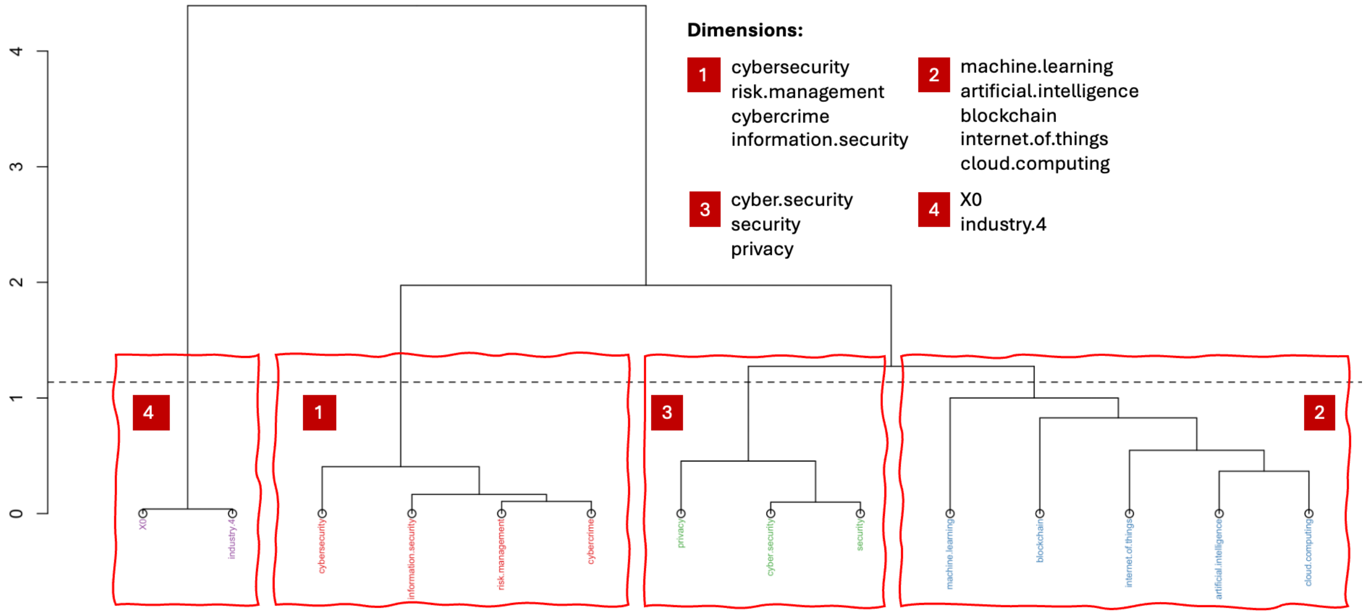


Figure 13
Dendrogram of words
Source: Own elaboration based on Aria and Cuccurullo (2017) and Clarivate (2023).

First, height measures the distance between words or groups of words. For this reason, the height of dimension 4 is more significant than 4.07, which confirms the distance from the other dimensions. For instance, a study found that robots and cybersecurity are the most used Industry 4.0 technologies worldwide, with different companies using them to increase efficiency or balance productivity with environmental sustainability. However, there is potential for more effective global adoption to drive sustainability-focused business models (Calabrese *et al.*, 2023).

Second, the height helps to choose where to cut the dendrogram that defines the partition. In this case, the dendrogram's height of 1.12 defines the four dimensions. Third, the distant words define a different concept or topic, and the dendrogram shows that the words of dimension 4 are more distant from dimension 2. Lastly, similar words explain a similar concept or topic, verified, for example, in dimension 3 (privacy, cyber security, and security), confirming the strong relationship between the three topics.

In summary, factor analysis helped understand the underlying structure of a framework by analyzing word associations within a network and reduced the complexity of the data by defining four dimensions. In this way, the results can help academics, policymakers, and business decision-makers in cybersecurity management.

5. DISCUSSION

This section discusses the main results of the bibliometric review on cybersecurity and business.

The study revealed an expressive growth in scientific production from 2018, and it shows the academic interest in these topics and the need to respond to a growing concern in most organizations (Kappelman *et al.*, 2022). The results also revealed "security" among the top ten most occurring words, which agrees with other researchers in recommending that companies in the energy sector should prepare for existing and emerging dangers and threats, including cyber-attacks (Kosmowski *et al.*, 2022). This outcome also responds to another study that showed that essential security vulnerabilities in IoT environments were worth highlighting (Hayat *et al.*, 2022).

The indicator of global trends over time revealed "information", "innovation", and "trust" as the main ones in 2023. This result converges with other authors who indicated that Industry 4.0 could be used more effectively globally despite its potential to drive business models focused on sustainability (Calabrese *et al.*, 2023). Furthermore, this finding responds to researchers who warned about the scarcity of applicable and detailed models at lower levels to manage cybersecurity (Manuel *et al.*, 2022). In this regard, the research proposes a model with a methodology to manage lower-level cybersecurity (Manuel *et al.*, 2022).

The bibliometric study has not only allowed us to identify the most cited articles, but also to uncover novel solutions for cybersecurity. For instance, research has proposed a unique framework for predictive manufacturing cyber-physical systems with IoT and Big Data analytics capabilities (Babiceanu & Seker, 2016). This finding is a direct response to concerns raised by other researchers about real-time security breaches in industrial platforms the need to identify critical assets for protection against cyberattacks (Bhamare *et al.*, 2020), and the evaluation of commercial impacts (Corallo *et al.*, 2023). Another study has underscored the potential of AI in promoting environmental governance (Nishant *et al.*, 2020), aligning with other research on reducing impacts on the Sustainable Development Goals (SDGs) (Marti & Cervelló-Royo, 2023). Lastly, researchers have suggested a distributed deep learning scheme for detecting cyberattacks in cloud computing, which offers higher accuracy and scalability than traditional methods (Abeshu & Chilamkurti, 2018). These findings directly address concerns raised by other authors about privacy and security in healthcare (Paul *et al.*, 2023).

The thematic evolution analysis showed that the relevance of the study theme coincides with the research in which the authors indicate that adopting artificial intelligence and machine learning applied to cybersecurity requires the global partnership of industry, academia, and public administration (Bresniker *et al.*, 2019). The analysis of the thematic map revealed that the driving topics are blockchain, privacy, and cloud computing, as well as machine learning, deep learning, and intrusion detection, which are at the center of the diagram. These results respond to researchers who indicated that to address the threat, and organizations must develop situational awareness in their incident response practices (Ahmad *et al.*, 2021). Also, the thematic map coincides with findings from another research that reveal that advances in cybersecurity depend on the involvement of industry, academia, and public administration (Bresniker *et al.*, 2019). Finally, the result confirms that one of the industrial sector's biggest challenges is understanding the risks posed by potential cyber-attacks (Kosmowski *et al.*, 2022). In summary, these results reduce the first knowledge gap on the need to generate awareness as an organizational response to incidents (Ahmad *et al.*, 2021) and understand the cyber risks they are exposed to (Kosmowski *et al.*, 2022).

The theoretical background indicated several causes and effects connected to cybersecurity and business. For example, one research mentioned that cyberattacks could generate a loss of productivity, a lack of customer trust, and legal sanctions (Ahmad *et al.*, 2021). Another research indicated that cybercrime cases constantly increase in online e-banking (Ngoc Thach *et al.*, 2021). The same research showed that cyber risk could affect brand, reputation, competitiveness, and financial value (Ngoc Thach *et al.*, 2021), and another study on business sustainability (Kosmowski *et al.*, 2022). These findings help raise awareness among decision-makers about the risks that companies may be exposed to and the consequences of not adequately managing this issue. Other research has shown solutions to reduce the mentioned problems and improve business management. For example, organizations need to invest in cybersecurity and improve technology management (Ngoc Thach *et al.*, 2021). Technological solutions require more advanced and collaborative approaches (Rashid *et al.*, 2021). Additionally, the industrial sector needs to understand cyber-attack risks when adopting technologies (Kosmowski *et al.*, 2022).

This paper is novel in conducting a bibliometric review on cybersecurity and business, which reduces the second identified knowledge gap. The results of the indicators (scientific production, keyword analysis, publication analysis, author analysis, and conceptual structure analysis) respond to RQ_1 by presenting the knowledge base on cybersecurity and business and its intellectual structure. On the other hand, the results of the indicators (production by countries, analysis by institutions, journal analysis, and cross-country collaboration) respond to RQ_2 by showing the cybersecurity and business research front.

6. LIMITATIONS AND FUTURE RESEARCH

This research provides an overview of the current bibliometric landscape in cybersecurity and business. However, some limitations should be acknowledged.

First, the findings are subject to change over time. As a result, these conclusions may evolve with the increasing popularity of new variables in the future.

Second, this study adheres to the methodologies used by WoS. Consequently, the limitations associated with these databases also apply to this work. For example, WoS implements a complete count, meaning that articles written by multiple people have a more significant impact than those with a single author. This research employs fractional counting in visual mapping using Biblioshiny to address this issue. However, more comprehensive methods will be necessary in the future.

Third, it is essential to acknowledge that the findings of this paper are strongly influenced by popularity and related factors. While this approach effectively identifies salient trends, it is critical to understand that other valuable research may not yield equally favorable results due to topic-specific characteristics such as a smaller research community or concepts that have not yet gained significant traction among scholars publishing in academic journals.

Fourth, the research only considered articles in English. Future studies may include research in other languages and publications such as books, book chapters, and conference proceedings.

Fifth, using WoS as a database alone may be a limitation. Despite justifying this choice for this research, future studies may consider other databases such as Scopus and Dimensions.

Finally, there are opportunities to deepen business research, with particular emphasis on information, innovation, and trust. Future lines of research can explore multi-criteria decision-making models and fuzzy logic to reduce uncertainty and cyber-attacks. Along these lines, future studies can propose management models that increase cybersecurity in companies and, at the same time, reduce uncertainty and risks in decision-making. Therefore, a promising field of research opens that may include Multi Criteria Decision-Making (MCDM) (Blanco-Mesa *et al.*, 2017) and Fuzzy Logic models (Barcellos-Paula *et al.*, 2022), such as, for example, the "Forgotten Effects Theory" (Kaufmann & Gil-Aluja, 1988) as a relationship algorithm, the "Affinities Theory" (Gil-Aluja, 1999) as a grouping algorithm; and the "OWA Operator" (Yager, 1988) as a sorting algorithm.

7. CONCLUSIONS

The research identified the knowledge base on cybersecurity and business and its intellectual structure and provided insight into the scientific progress in this discipline. The authors used the WoS database and Bibliometrix software to analyze 410 articles and 1,355 authors across nine bibliometric indicators between 2004 and 2023. The theoretical background also identified knowledge gaps and broadened the discussion on cybersecurity and business.

The main results revealed an upward trend in publications with an annual growth of 27.63% and 31.46% international co-authorship, reinforcing the academic interest in cybersecurity and business to reduce a growing concern of organizations. The research indicated that the USA has the highest scientific output, followed by the UK and China. The study showed that "security" is the most used keyword in research. Other findings revealed Business Horizons and IEEE Access as the top journals and authors Kappelman, Maurer, and Torres as the most relevant. Top affiliations were Indiana University System, Indiana University Bloomington, and State University System of Florida. The thematic mapping revealed that the driving topics are blockchain, privacy, and cloud computing. Therefore, researchers can deepen studies in this field. Finally, the factorial analysis confirmed that cybersecurity, cybercrime, risk management, and information security are the most common and significant topics shared.

As theoretical contributions, the study advanced the frontier of knowledge by narrowing the gaps identified to minimize cyber risks and analyzing security management. Likewise, the bibliometric review made it possible to determine the intellectual structure and to learn about the research front on cybersecurity and business. The study also showed promising lines of research. Finally, the study presented a bibliometric review methodology that other researchers can apply.

As practical contributions, the research broadened the debate on cybersecurity and business, seeking to raise decision-makers awareness of the risks to which companies may be exposed and find solutions for better business management. In addition, the study showed the terms most associated with cybersecurity and business, which can improve the analysis of managers and policymakers in decision-making and cybersecurity management.

Finally, the study's main scientific merit is its innovation. It conducted a bibliometric review on cybersecurity and business using a combined approach, including scientific mapping and performance analysis, with 410 articles and nine bibliometric indicators. Additionally, the authors sought to raise awareness among decision-makers about the links between cybersecurity and business.

8. ACKNOWLEDGMENT

Research supported by Red Sistemas Inteligentes y Expertos Modelos Computacionales Iberoamericanos (SIEMCI), project number 522RT0130 in the Ibero-American Science and Technology for Development Program (CYTED).

9. REFERENCES

Abeshu, A., & Chilamkurti, N. (2018). Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing. *IEEE Communications Magazine*, *56*(2), 169–175. https://doi.org/10.1109/MCOM.2018.1700332

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

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144–166. https://doi.org/10.1016/j.cose.2018.01.001

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

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*. https://doi.org/10.1016/j.comnet.2019.106946

Babiceanu, R. F., & Seker, R. (2016). Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. *Computers in Industry*, *81*, 128–137. https://doi.org/10.1016/j.compind.2016.02.004

Barcellos-Paula, L., de La Vega, I., & Gil-Lafuente, A. M. (2022). Bibliometric review of research on decision models in uncertainty, 1990–2020. *International Journal of Intelligent Systems*, *37*(10), 7300–7333. https://doi.org/10.1002/int.22882

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, *89*, 101677. https://doi.org/10.1016/j.cose.2019.101677

Blanco-Mesa, F., León-Castro, E., & Merigó, J. M. (2019). A bibliometric analysis of aggregation operators. *Applied Soft Computing*, *81*, 105488. https://doi.org/10.1016/j.asoc.2019.105488

Blanco-Mesa, F., Merigó, J. M., & Gil-Lafuente, A. M. (2017). Fuzzy decision making: A bibliometric-based review. *Journal of Intelligent & Fuzzy Systems*, *32*(3), 2033–2050. https://doi.org/10.3233/JIFS-161640

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7). https://doi.org/10.1016/j.technovation.2014.02.001

Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., & Tran, T. (2019). Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity. *Computer*, *52*(12), 45–52. https://doi.org/10.1109/MC.2019.2942584

Broadus, R. N. (1987). Early approaches to bibliometrics. *Journal of the American Society for Information Science*, *38*(2). https://doi.org/10.1002/(SICI)1097-4571(198703)38:2<127::AID-ASI6>3.0.CO;2-K

Calabrese, A., Costa, R., Tiburzi, L., & Brem, A. (2023). Merging two revolutions: A human-artificial intelligence method to study how sustainability and Industry 4.0 are intertwined. *Technological Forecasting and Social Change*, *188*. https://doi.org/10.1016/j.techfore.2022.122265

Chaal, M., Ren, X., BahooToroody, A., Basnet, S., Bolbot, V., Banda, O. A. V., & Gelder, P. Van. (2023). Research on risk, safety, and reliability of autonomous ships: A bibliometric review. *Safety Science*, *167*, 106256. https://doi.org/10.1016/j.ssci.2023.106256

Clarivate (2023). Journal Citation Reports: Reference Guide. Journal Citation Reports.

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011a). An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field. *Journal of Informetrics*, *5*(1), 146–166. https://doi.org/10.1016/j.joi.2010.10.002

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011b). Science mapping software tools: Review, analysis, and cooperative study among tools. *Journal of the American Society for Information Science and Technology*, *62*(7), 1382–1402. https://doi.org/10.1002/asi.21525

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, *114*, 103165. https://doi.org/10.1016/j.compind.2019.103165

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, 103614. https://doi.org/10.1016/j.compind.2022.103614

Corallo, A., Lazoi, M., Lezzi, M., & Pontrandolfo, P. (2023). Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. *IEEE Transactions on Engineering Management*, *70*(11). https://doi.org/10.1109/TEM.2021.3084687

Garfield, E. (1955). Citation indexes for science. *Science*, *122*(3159). https://doi.org/10.1126/science.122.3159.108

Ghobakhloo, M. (2020). Determinants of information and digital technology implementation for smart manufacturing. *International Journal of Production Research*, *58*(8), 2384–2405. https://doi.org/10.1080/00207543.2019.1630775

Gil-Aluja, J. (1999). *Elements for a Theory of Decision in Uncertainty* (Vol. 32). Springer US. https://doi.org/10.1007/978-1-4757-3011-1

Gupta, S., Meissonier, R., Drave, V. A., & Roubaud, D. (2020). Examining the impact of Cloud ERP on sustainable performance: A dynamic capability view. *International Journal of Information Management*, *51*. https://doi.org/10.1016/j.ijinfomgt.2019.10.013

Hasanova, H., Baek, U. jun, Shin, M. gon, Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2). https://doi.org/10.1002/nem.2060

Hayat, R. F., Aurangzeb, S., Aleem, M., Srivastava, G., & Lin, J. C. W. (2022). ML-DDoS: A Blockchain-Based Multilevel DDoS Mitigation Mechanism for IoT Environments. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2022.3170519

Hayes, A. (2020). Business Definition. *Investopedia*.

Hosseini Shirvani, M., Rahmani, A. M., & Sahafi, A. (2018). An iterative mathematical decision model for cloud migration: A cost and security risk approach. *Software - Practice and Experience*, *48*(3). https://doi.org/10.1002/spe.2528

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health Care and Cybersecurity: Bibliometric Analysis of the Literature. *Journal of Medical Internet Research*, *21*(2), e12644. https://doi.org/10.2196/12644

Javaheri, D., Gorgin, S., Lee, J. A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. *Information Sciences*, *626*. https://doi.org/10.1016/j.ins.2023.01.067

Johnson, M. E., Goetz, E., & Pfleeger, S. L. (2009). Security through information risk management. *IEEE Security and Privacy*, *7*(3). https://doi.org/10.1109/MSP.2009.77

Johnson, V., Torres, R., Maurer, C., Guerra, K., Srivastava, S., & Mohit, H. (2023). The 2022 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, *22*(1). https://doi.org/10.17705/2msqe.00075

Kappelman, L., Johnson, V., Maurer, C., McLean, E., Torres, R., David, A., & Nguyen, Q. (2018). The 2017 SIM IT issues and trends study. *MIS Quarterly Executive*, *17*(1).

Kappelman, L., Johnson, V., Torres, R., Maurer, C., & McLean, E. (2019). A study of information systems issues, practices, and leadership in Europe. *European Journal of Information Systems*, *28*(1). https://doi.org/10.1080/0960085X.2018.1497929

Kappelman, L., Maurer, C., Mclean, E. R., Kim, K., Johnson, V. L., Guerra, K., Torres, R., & Snyder, M. (2021). The 2020 SIM IT Issues and Trends Study. *MIS Quarterly Executive, 20*(1).

Kappelman, L., Torres, R., McLean, E., Maurer, C., Johnson, V., & Kim, K. (2018). The 2018 SIM IT issues and trends study. *MIS Quarterly Executive*, *18*(1). https://doi.org/10.17705/2msqe.00008

Kappelman, L., Torres, R., McLean, E. R., Maurer, C., Johnson, V. L., Snyder, M., & Guerra, K. (2022). The 2021 SIM IT Issues and

Trends Study. *MIS Quarterly Executive*, *21*(1), 75–114. https://doi.org/10.17705/2msqe.00060

Kaufmann, A. & Gil-Aluja, J. (1988). *Modelos para la investigación de efectos olvidados*. Editorial Milladoiro.

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice*, *37*(4), 480–501. https://doi.org/10.1177/10439862211027986

Khan, A. A., Uddin, M., Shaikh, A. A., Laghari, A. A., & Rajput, A. E. (2021). MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3099037

Klaus, J. P., Kim, K., Masli, A., Guerra, K., & Kappelman, L. (2022). Prioritizing IT Management Issues and Business Performance. *Journal of Information Systems*, *36*(2). https://doi.org/10.2308/ISYS-2020-016

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

Kosmowski, K. T., Piesik, E., Piesik, J., & Śliwiński, M. (2022). Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. *Energies*, *15*(10), 3610. https://doi.org/10.3390/en15103610

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

Leng, J., Ye, S., Zhou, M., Zhao, J. L., Liu, Q., Guo, W., Cao, W., & Fu, L. (2021). Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *51*(1), 237–252. https://doi.org/10.1109/TSMC.2020.3040789

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Manuel, D.-D., Carmona-Murillo, J., Cortes-Polo, D., & Rodriguez-Perez, F. J. (2022). CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels. *IEEE Access*, *10*, 122454–122485. https://doi.org/10.1109/ACCESS.2022.3223440

Marti, L., & Cervelló-Royo, R. (2023). Disparities in sustainable development goals compliance and their association with country risk. *Sustainable Development*. https://doi.org/10.1002/sd.2568

Martínez-López, F. J., Merigó, J. M., Valenzuela-Fernández, L., & Nicolás, C. (2018). Fifty years of the European Journal of Marketing: a bibliometric analysis. In *European Journal of Marketing* (Vol. 52, Issues 1–2). https://doi.org/10.1108/EJM-11-2017-0853

Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. *Enterprise Information Systems*, *15*(4). https://doi.org/10.1080/17517575.2019.1600041

Moed, H. F. (2005). Citation Analysis in Research Evaluation (Information Science and Knowledge Management). In *Analysis*.

Naffa, H., & Fain, M. (2020). Performance measurement of ESG-themed megatrend investments in global equity markets using pure factor portfolios methodology. *PLOS ONE*, *15*(12), e0244225. https://doi.org/10.1371/journal.pone.0244225

Ngoc Thach, N., Thanh Hanh, H., Ngoc Huy, D. T., Gwozdziewicz, S., Viet Nga, L. T., & Thanh Huong, L. T. (2021). Technology Quality Management of the Industry 4.0 and Cybersecurity Risk Management on Current Banking Activities in Emerging Markets - The Case in Vietnam. *International Journal for Quality Research*, *15*(3), 845–856. https://doi.org/10.24874/IJQR15.03-10

Nishant, R., Kennedy, M., & Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. *International Journal of Information Management*, *53*, 102104. https://doi.org/10.1016/j.ijinfomgt.2020.102104

Noyons, E. C. M., Moed, H. F., & Luwel, M. (1999). Combining mapping and citation analysis for evaluative bibliometric purposes: A bibliometric study. *Journal of the American Society for Information Science*, *50*(2), 115–131. https://doi.org/10.1002/(SICI)1097-4571(1999)50:2<115::AID-ASI3>3.0.CO;2-J

Page MJ, McKenzie JE, Bossuyt PM, et al (2021) The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. The BMJ 372:71.

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. In *ICT Express* (Vol. 9, Issue 4). https://doi.org/10.1016/j.icte.2023.02.007

Pedraja-Rejas, L., Rodríguez-Ponce, E., & Muñoz-Fritis, C. (2022). Human resource management and performance in Ibero-America: Bibliometric analysis of scientific production. *Cuadernos de Gestion*, *22*(2). https://doi.org/10.5295/cdg.211569lp

Pritchard, A. (1969). Statistical Bibliography or Bibliometrics? In *Journal of Documentation* 25 (4): 348-349.

Protogerou, A., Papadopoulos, S., Drosou, A., Tzovaras, D., & Refanidis, I. (2021). A graph neural network method for distributed anomaly detection in IoT. *Evolving Systems*, *12*(1). https://doi.org/10.1007/s12530-020-09347-0

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

Ribeiro, H., Barbosa, B., Moreira, A. C., & Rodrigues, R. (2022). Churn in services – A bibliometric review. *Cuadernos de Gestion*, *22*(2). https://doi.org/10.5295/cdg.211509hr

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*(4). https://doi.org/10.1016/j.bushor.2012.02.004

Shah, S. (2020). The Technological Impact of COVID-19 on the Future of Education and Health Care Delivery. *Pain Physician*, *4S;23*(8;4S), S367–S380. https://doi.org/10.36076/ppj.2020/23/S367

Silva, B. C., & Moreira, A. C. (2022). Entrepreneurship and the gig economy: A bibliometric analysis. *Cuadernos de Gestion*, *22*(2). https://doi.org/10.5295/cdg.211580am

Tagarev, T., Davis, B., & Cooke, M. (2022). Business, Organisational and governance modalities of collaborative cybersecurity networks. *Multimedia Tools and Applications*, *81*(7). https://doi.org/10.1007/s11042-021-11109-2

Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber Risk Assessment and Optimization: A Small Business Case Study. *IEEE Access*, *11*. https://doi.org/10.1109/ACCESS.2023.3272670

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *SCIENTOMETRICS*, *84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Yager, R. R. (1988). On ordered weighted averaging aggregation operators in multicriteria decisionmaking. *IEEE Transactions on Systems, Man, and Cybernetics*, *18*(1), 183–190. https://doi.org/10.1109/21.87068

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3087109

Zupic, I., & Čater, T. (2015). Bibliometric Methods in Management and Organization. *Organizational Research Methods*, *18*(3), 429–472. https://doi.org/10.1177/1094428114562629