Revista Ibero-Americana de Estratégia
Iberoamerican Journal of Strategic Management

COPE JM14473

e-ISSN: 2176-0756
https://doi.org/10.5585/2023.23846
Received: 15 Feb. 2023 / **Approved:** 16 June 2023
Evaluation Process: Double Blind Review
Editor in Chief: Heidy Rodriguez Ramos
Coeditor: Ivano Ribeiro
Section Editor: Dra. Nairana Radtke Caneppele
Assistant Editor: Leandro Rodrigues de Oliveira

Check for updates

BIBLIOMETRIC ANALYSIS OF PUBLICATIONS ON CYBER RISKS IN THE SERVICES SECTOR

Marcia C. Rossi [1] **Gilberto Perez** [2]

Objective: To explore the progress of scientific production on cyber risks that permeate the service sector, identifying relevant researchers and institutions on this theme, measuring the impact, and identifying trends, contributions, and knowledge gaps. In addition, the study seeks to use bibliometric findings to bring academic and managerial contributions to the subject.
Methodology: Bibliometric study, using the method of organization and systematization of information (Chueke & Amatucci, 2015; Guedes & Borschiver, 2015), whose structure followed the premises of the laws of Bradford, Lotka, and Zipf, using the scientific databases of the WoS - Web of Science. The bibliometric study enabled the performance of exploratory and descriptive research without the temporal cut, resulting in the identification of 115 publications (December 1995 to February 2023), which allowed measuring and presenting the characteristics and profile of the publications analyzed.
Originality: The study revealed a potential for exploring the theme of Cyber Risks in the Services sector, considering the scarcity of scientific production. It also enabled the identification of emerging trends and clusters in service sector activities and the creation of a conceptual model based on the findings of the analyzed publications.
Main results: The analyses revealed which sectors of the service economy are most frequently approached in publications related to the theme of cyber risks. These analyses were organized into ten areas, with the following order of relevance (frequency) of publication: Computer Science, Information Systems, Engineering, Business, Finance and Management, Telecommunications, Computer Science Theory Methods, and Computer Science Artificial Intelligence. The bibliometric findings enabled the creation of the conceptual model of Cyber Risks in Services, which proposes a cyclical and continuous improvement approach to deal with vulnerabilities, cyber threats, and consequences. This includes identifying and assessing existing vulnerabilities, implementing mitigation measures, and constantly monitoring threats and their consequences.
Theoretical contributions: The conceptual model of Cyber Risks in Services can be a reference for researchers in various fields of action, considering the breadth of the services sector and the interdisciplinary nature of digital risk mitigation.
Managerial contributions: Understanding of cyber risks supports the ability of the organization to respond to them, strengthening its security posture and protecting its critical assets and information from cyber threats.

Keywords: Bibliometry, Cyber Risks. Services Sector.

ANÁLISE BIBLIOMÉTRICA DAS PUBLICAÇÕES SOBRE RISCOS CIBERNÉTICOS NO SETOR DE SERVIÇOS

Objetivo: Explorar o avanço da produção científica sobre os riscos cibernéticos que permeiam o setor de serviços, identificando pesquisadores e instituições relevantes no tema, medindo o impacto e identificando tendências, contribuições e lacunas de conhecimento. Além disso, o estudo busca utilizar achados bibliométricos para trazer contribuições acadêmicas e gerenciais para o tema.
Metodologia: Estudo bibliométrico, utilizando o método de organização e sistematização da informação (Chueke & Amatucci, 2015; Guedes & Borschiver, 2015), cuja estrutura seguiu as premissas das leis de Bradford, Lotka e Zipf, utilizando as bases de dados científicas da WoS - Web of Science. O estudo bibliométrico possibilitou a realização de pesquisa exploratória e descritiva sem recorte temporal, resultando na identificação de 115 publicações (dezembro de 1995 a fevereiro de 2023), o que permitiu mensurar e apresentar as características e o perfil das publicações analisadas.
Originalidade: O estudo revelou potencial para explorar o tema Riscos Cibernéticos no setor de Serviços, considerando a escassez de produção científica. Também permitiu a identificação de tendências emergentes e clusters nas atividades do setor de serviços e a criação de um modelo conceitual com base nas conclusões das publicações analisadas.
Principais resultados: As análises revelaram quais setores da economia de serviços são mais abordados em publicações relacionadas ao tema dos riscos cibernéticos. Essas análises foram organizadas em dez áreas, com a seguinte ordem de relevância (frequência) de publicação: Ciência da Computação, Sistemas de Informação, Engenharia, Negócios, Finanças e Gestão, Telecomunicações, Métodos da Teoria da Ciência da Computação e Inteligência Artificial da Ciência da Computação. Os achados bibliométricos permitiram a criação do modelo conceitual de Riscos Cibernéticos em Serviços, que propõe uma abordagem de melhoria cíclica e contínua para lidar com vulnerabilidades, ameaças cibernéticas e consequências. Isso inclui identificar e avaliar as vulnerabilidades existentes, implementar medidas de mitigação e monitorar constantemente as ameaças e suas consequências.
Contribuições teóricas: O modelo conceitual de Riscos Cibernéticos em Serviços pode ser uma referência para pesquisadores em diversas áreas de atuação, considerando a amplitude do setor de serviços e a natureza interdisciplinar da mitigação de riscos digitais.
Contribuições gerenciais: A compreensão dos riscos cibernéticos apóia a capacidade da organização de responder a eles, fortalecendo sua postura de segurança e protegendo seus ativos e informações críticas de ameaças cibernéticas.

Palavras-chave: Bibliometria. Riscos Cibernéticos. Setor de Serviços.

ANÁLISIS BIBLIOMÉTRICO DE PUBLICACIONES SOBRE CIBERRIESGOS EN EL SECTOR SERVICIOS

Objetivo: Explorar el avance de la producción científica sobre los ciberriesgos que permean el sector servicios, identificando investigadores e instituciones relevantes en la materia, así como medir el impacto e identificar tendencias, aportaciones y lagunas de conocimiento. Además, el estudio pretende utilizar los resultados bibliométricos para aportar contribuciones académicas y de gestión sobre el tema.
Metodología: Estudio bibliométrico, utilizando el método de organización y sistematización de la información (Chueke & Amatucci, 2015; Guedes & Borschiver, 2015), cuya estructura siguió las premisas de las leyes de Bradford, Lotka y Zipf, utilizando las bases de datos científicas de WoS - Web of Science. El estudio bibliométrico permitió la realización de una investigación exploratoria y descriptiva sin corte temporal, resultando en la identificación de 115 publicaciones (diciembre de 1995 a febrero de 2023), lo que permitió medir y presentar las características y el perfil de las publicaciones analizadas.
Originalidad: El estudio reveló un potencial para explorar el tema del Ciberriesgo en el sector Servicios, dada la escasez de producción científica. Además, permitió identificar tendencias y clusters emergentes en las actividades del sector servicios y crear un modelo conceptual a partir de las conclusiones de las publicaciones analizadas.
Principales resultados: Los análisis revelaron qué sectores de la economía de servicios se abordan con mayor frecuencia en las publicaciones relacionadas con el tema de los ciberriesgos. Estos análisis se organizaron en diez áreas, con el siguiente orden de relevancia (frecuencia) de publicación: Informática, Sistemas de Información, Ingeniería, Negocios, Finanzas y Gestión, Telecomunicaciones, Métodos Teóricos de la Informática e Inteligencia Artificial de la Informática. Los resultados bibliométricos permitieron crear el modelo conceptual de Ciberriesgos en los Servicios, que propone un enfoque cíclico y de mejora continua para hacer frente a las vulnerabilidades, las ciberamenazas y sus consecuencias. Esto incluye la identificación y evaluación de las vulnerabilidades existentes, la implementación de medidas de seguridad para mitigarlas y el monitoreo constante de las amenazas y sus consecuencias.
Aportes teoricos: El modelo conceptual de Riesgos Cibernéticos en los Servicios puede ser una referencia para los investigadores en diversos campos de actividad, teniendo en cuenta la amplitud del sector servicios y la naturaleza interdisciplinaria de la mitigación del riesgo digital.
Aportes gerenciales: Comprensión de los riesgos cibernéticos ayuda a la organización a responder a ellos, reforzando su postura de seguridad y protegiendo sus activos e información críticos frente a las ciberamenazas.

Palabras clave: Bibliometría. Ciberriesgos. Sector Servicios.

Cite as / Como citar

American Psychological Association (APA)

Rossi, M. C., & Perez, G. (2023). Bibliometric analysis of publications on cyber risks in the services sector. *Iberoamerican Journal of Strategic Management (IJSM), 22*(1), 1-25, e23846. https://doi.org/10.5585/2023.23846

(ABNT – NBR 6023/2018)

ROSSI, Márcia. C.; PEREZ, Gilbetto. Bibliometric analysis of publications on cyber risks in the services sector. *Iberoamerican Journal of Strategic Management (IJSM),* v. 22, n. 1, p. 1-25, e23546, 2023. https://doi.org/10.5585/2023.23846

[1] Researcher in Resources and Business Development. Master's degree in Controllership. Professor of specialization courses in Financial Controlling and MBA programs in Strategic Business Management at Universidade Presbiteriana Mackenzie, SP. São Paulo/SP – Brazil contato@marciarossi.com (Principal contact for editorial correspondence)

[2] Associate Professor from the University of São Paulo (USP/FEA, 2022). Adjunct Professor of the Stricto Sensu Graduate Program in Administration (PPGA) at Universidade Presbiteriana Mackenzie. São Paulo/SP – Brazil. gperez@mackenzie.br

1 Introduction

The digitization processes of the economy and society have been important for the growth and continuity of companies, with a potentially significant impact on global prosperity. Information and communication technologies have increased their rates of sharing, storing, and processing personal information at an exponential level (Conger, Pratt, & Loch, 2012, Saridakis, Benson, Ezingeard, & Tennakoon, 2016). Incidents such as cyber risks have brought relevant economic and social implications or significant impact on public safety (Mantha & Soto, 2020).

The impact of digitization on business processes has encouraged transformation markets to create or improve products, services, and relational modalities (Barile, Grimaldi, Loia, & Sirianni, 2020). At the same time, another active front has progressively explored new business models, driven by companies looking for new replacements and adopting strategies that meet their customers' needs.

In this sense, the challenges of servitization have increasingly attracted the attention of companies in the industrial sector, which seek, in planning, the comprehensive service strategy, a current service category that exposes numerous opportunities with positive perspectives to the same extent that risks are jointly neglected (Fang, Palmatier, & Steenkamp, 2008, Nordin, Kindström, Kowalkowski, & Rehme, 2011; Rajapathirana & Hui, 2018, Raddats, Kowalkowski, Benedettini, Burton, & Gebauer, 2019).

Cyberspace is not just the internet, including hardware, software, and information systems, and it also involves people and their interactions in computer networks, whether commercial or not (Klimburg, 2012; Silva & Nogueira, 2019). The customer's presence as a participant in the service process requires attention to facility design, which, until recently, was not optional for traditional manufacturing operations (Fitzsimmons & Fitzsimmons, 2014).

A theoretical gap between cyber risks and the service sector lies in the lack of a comprehensive model or framework that integrates the specifics of cyber risks with the challenges faced by the service sector. Although there are discussions about cybersecurity and various frameworks and models for assessing and mitigating digital risks, applying these concepts to the service sector can be complex and challenging. The service economy is not limited to a single entity but encompasses a wide range of services with diverse business models. It encompasses various activities that offer varied services, each with its particularities regarding how they operate, compete, and are regulated (Gallouj, 2023; Metters, 2023).

Given this scenario, exploring the literature and the works developed on the subject is proposed. This research aims to answer the following question: **What is the profile of the scientific production that has approached cyber risks in the service sector?** To answer the proposed question, a bibliometric study was conducted using the method of organizing and systematizing information proposed by Chueke and Amatucci (2015). The structure of the research followed the premises of the laws of Bradford, Lotka, and Zipf, using the scientific databases of the Web of Science (WoS).

Furthermore, this study seeks to use the bibliometric findings as the basis for building a conceptual model that expands the understanding of the research area.

It is necessary to explore cyber risks discussions about the service sector, which plays a crucial role in permeating the supply of products and goods. Understanding cyber risk not only assists companies in ensuring and managing compliance in their processes, avoiding potential financial penalties, third-party damages, and reputational damage but also makes academic contributions by filling a knowledge gap on the specific challenges faced by the service sector in this context. Analyzing cyber risks in the services sector at the policy-legal level can support formulating appropriate policies and regulations to protect sensitive data and ensure cybersecurity. Moreover, this understanding contributes to increase awareness of the importance of privacy protection, consumer trust, and digital inclusion, promoting a holistic view to approach the social and ethical impacts of digitalization and automation in the service industry.

To achieve the proposed objective, this paper is organized into five sections. Distinguishing the introduction and the conclusion, Section Two begins by exploring the concepts of cyber risk, highlighting the threats and vulnerabilities that organizations have faced. Risk management strategies, data protection, and cybersecurity are addressed in this context. Also, the service sector and its relevance in the economy are addressed. Strategies for growth, innovation, and customer satisfaction (and participation) in this constantly evolving industry are exposed. The combination of these two topics aims to provide a comprehensive understanding of a scenario in which organizations face cyber challenges and seek an appropriate balance between innovation and security in services. The third section presents the methodological approach adopted to develop this study. The fourth section presents the results obtained, including the service sectors identified in the analysis of the articles. The most frequently used keywords will help highlight the sector's tendency to face digital risks, the most cited articles and authors, and the countries of origin of the publications, which help visualize the focus of development and investments in research on this theme. The fifth section, which precedes the Final Remarks Section, discusses the results obtained, combining them with the theoretical background.

2 Theoretical Reference

Given the increasing reliance on digital technologies in service-related activities, understanding the nature and implications of cyber risks has become fundamental for researchers and managers alike. Before exploring the profile of the scientific production that addresses cyber risks in the services sector through bibliometrics, this theoretical framework sought to provide a comprehensive understanding of the existing knowledge in this area through a literature review. This review allowed for a brief exploration of the concepts related to cyber risks and the services sector.

2.1 Cyber Risks

Cybernetics originates from Greek, meaning the "art of the pilot" (Abbagnano, 2007), leading to understanding control and direction. The term stood out during the works and experiments related to the Second World War by the mathematician Norbert Wiener, which helped him publish "Cybernetics: or control and communication in the animal and the machine" in 1948 (Wiener, 2017). This work develops and presents the hypotheses of this theme, arising from research and multidisciplinary interaction with other scientific groups, formed by mathematicians, physicists, engineers, and social scientists.

Cybernetics is a pluralistic and interdisciplinary area of scientific knowledge (Kim, 2004, Kandjani, Wen, & Bernus, 2012). However, Wiener belatedly discovered that Ampère had already used the same word about political science (Wiener, 1984). The development of cybernetics induced scientists to develop new and complex mathematical models to expand the man-machine system. Words commonly cited with the prefix cyber, such as cyberspace, owe their origin to cybernetics, which inaugurated many developments (Kandjani et al., 2012).

Pierre Lévy (2000) considered the study of cyberspace as a science of information and communication, understanding that cyberspace is a means of communication arising from the global network of interconnected computers, not specifically the physical structure of digital communication, but its use by people that seek, promote and feedback a multitude of information through this mechanism. This perspective reinforces one of the main points attributed to cybernetics: there is no discontinuity between machines and men, whose exchange depends on functional compatibility (Kim, 2004).

Cyber risk is considered a sub-risk of operational risks for information and technology assets and can affect the confidentiality, availability, and integrity of the information or system (Cebula & Young, 2010). Risks can take two forms: a) a static or pure nature, characterized by the risk of loss; b) of a speculative or dynamic nature, which involves the possibility of a loss by one of the parties, while the other gains some gain (Powers, 2006; Durak, 2020).

For Neghina and Scarlat (2012), organizations should advocate the transition from an approach based primarily on security to a closer approach to risk assessment, thus addressing vulnerabilities in risk management planning and methods.

In parallel, the high competitiveness in the market has forced organizations to improve their positioning concerning innovation and emerging technologies, and researchers have been unfolding themselves in exploring, analyzing, and conceptualizing the theme, according to the studies listed in Table 1:

Table 1

Main concepts of Cyber Risks

Authors	Concept	Focus
Brewer (2000)	Vulnerability can be measured by the multiplication of threat versus asset value.	Asset measurement, threat, and assets value
NIST (2006)	Negative impact on the organization's operation, involving informal elements based on mission, image, and reputation, in which resources and intellectual capital are the "means" of using the information system.	Potential, organizational operations and assets
World Economic Forum (2012)	It is a combination of the probability of an event in network information systems and the effects of that event on the assets and on the reputation of an organization.	Combination of probability, event, assets
Nieuwesteeg, Visscher & de Waard (2018)	The one that causes physical damage or impacts financial losses when there is a malfunction in the digital environment or when data are neglected or illegally shared.	Physical damage, financial loss, illegalities
Biener, Eling &Wirfs (2015)	Risk can be defined as a function of three parameters: 1) Impact expresses the level of damage that a given risk can cause. 2) Threat expressed whether a particular risk is probable. 3) Vulnerability expresses whether information security measures are effective or not.	Level of harm, expressed threat and vulnerability
NAIC (2018)	Risk related to a malicious electronic event which may cause business discontinuity and financial loss. It can be considered the one that covers all other risks associated with online activity, such as the storage of personal data and transactions that can result in image damage, financial loss, and adversity in life and business.	Business discontinuity, malicious event, adversities in life and business
Böhme, Laube & Riek (2018)	Two aspects can highlight cyber risks: 1) technical: process flow, reprogrammable behavior, and dynamic global threat; and 2) economic: information asymmetry, externalities, and common risk factors in operationalization.	Technical and economic aspects
Egan *et al.* (2019)	The risk depends on the malicious (or non-malicious) threats the organization faces and how it mitigates the risks through business and strategic decisions.	Threat, business decisions and strategies
Strupczewski (2021)	Cyber risks are linked to company security: remote work, teleworking, access to strategic and sensitive information, and careless use of equipment such as notebooks and smartphones.	Remote work, resources synced with company systems, and carelessness
Liu et *al.*, 2022	[…] taking advantage of vulnerabilities induced by the technology, hyper-connected systems, human-enabled errors, and organizations not prepared to prevent or counter such attacks.	Hyper-connected, human-enabled errors

Source: Based on the researched literature (2023)

Cyber risk is a recent scientific discussion, and its diversity and complexity have characterized an exponential change in cybersecurity and cyber threats. It has even gained focus from the accelerated digitization of the economy and interactions in cyber environment (Strupczewski, 2021).

Vulnerability can be measured by multiplying the threat by the value of assets, representing the potential negative impact on the operation of an organization, and expressing whether information security measures are effective. This impact encompasses tangible and intangible elements, such as reputation and use of resources, and the intellectual capital involved (Brewer, 2000; Biener et al., 2015; Liu et al., 2022).

Internet applications and services are increasingly vulnerable to attacks or information theft (Ghorbani & Ahmadzadegan, 2017). The concern with digital threats in cyber risks has remained in the background of the agenda of CEOs around the world. This finding is reinforced in studies, among them a survey carried out by Marsh in partnership with Microsoft, which involved 168 Brazilian companies in a total of 600 global companies, results of which revealed that 61% of these companies did not take out insurance with cyber risk coverage. While 22% could not answer whether the company invests in this type of insurance (Funke, 2021).

Companies have faced attacks from sophisticated groups, which have deployed malware, a type of malicious software directed against systems and individuals designed to harm or exploit any device, service, or programmable network (McAfee, 2021).

Assessing the damage caused by cyber-attacks has posed colossal and global challenges for businesses and governments. Attacks are known to cause catastrophic cascading service disruptions that have caused billions of dollars of financial loss to organizations and critical infrastructure worldwide (Pal et al., 2021). In 2020, amounts sent and received from illicit activities reached 10 billion dollars, representing 0,34% of the entire global operation with digital currencies (ChainAnalysis, 2020). Rosati, Gogolin, and Lynn (2022) point to deficiencies in internal organizational control, whose cybersecurity failures are considered significant risk factors which negatively affect companies' financial results.

In this sense, cyber risks include technical aspects such as process flow, reprogrammable behavior, dynamic global threats, and economic aspects such as information asymmetry, externalities, and shared operational risk factors (Böhme et al., 2018). The severity of these risks depends on the organization's ability to mitigate them through strategic and operational decisions (Egan et al., 2019).

As an aggravating factor, the COVID-19 pandemic has exposed new difficulties, in addition to the ones faced by the health area, such as the challenges caused by the flexibility of security of data and information, when, due to the remote work adopted by most companies, the organizational environment was extended to the individuals' home environment. The expansion of demand for services through applications is also worth mentioning, which grew 149% in 2020 (Saraiva, 2021). This demonstrates that consumers have increasingly resorted to requesting and using products and services through digital means.

Cyber risks are related to the enterprise's security, including remote working, telecommuting, access to strategic and sensitive information, and the responsible use of devices such as laptops and smartphones (Strupczewski (2021). These risks exploit vulnerabilities induced by technology, interconnected systems, human error, and organizations unprepared to prevent or deal with such attacks (Liu et al., 2022).

Managers should be aware of the various sources of cyber risk and their potential impact, ensuring that the business is sufficiently prepared against such events through security awareness of critical infrastructure entities through confidentiality, availability, and integrity of the services offered (Egan et al., 2019; Amanowicz & Kamola, 2022).

2.2 Services Sector

The service sector is a nomenclature recognized worldwide, based on a segment represented by the workforce since the industrial revolution, configuring itself as the co-production of values by people, technology, internal and external service system, and shared information (Fitzsimmons & Fitzsimmons, 2014).

Stoshikj, Kryvinska, & Strauss (2016, p. 214) summarize the sector as a "science of services composed of holistic service systems, such as cities, universities and hospitals – and which can be described as systems of systems, such as food, water, energy, health, education, transport", given that companies have competed to some degree based on services (Zeithaml, 2017).

In addition to the concepts and specificities brought by the service sector literature, plurality, intangibility (non-stock, non-transportability and, above all, non-transferability), and simultaneous consumption translate a practically unanimous format of the sector's performance (Gallouj, 1997; Mittal, 1999; Fitzsimmons & Fitzsimmons, 2014; Rajapathirana & Hui, 2018).

In Brazil, the representativeness of the service sector in the economy can be highlighted by the 74% share of service activities in the Gross Domestic Product (GDP) in 2020 (Agência Brasil, 2020). From a global perspective, Rubalcaba & Solano (2023) exposed the indicators that reflect the percentage share of services in total value added in development regions of the world, which reaches approximately 76%. Moreover, globally these services account for about 51% of employment.

In this content, the sector stands out in the 2030-Agenda for Sustainable Development, exposing the economy and trade of services with a great aptitude to induce structural transformations and development under the understanding that "national policies and regulatory efforts, as well as commercial policy, multilateral, regional and cooperative must recognize the potential for the development of services" (United Nations Conference, 2017).

On a large scale, "the economy as a whole can be interpreted as a huge system of services, containing a variety of interrelated entities and subsystems" (Stoshikj et al., 2016, p. 212). Even increasingly, outsourcing has been perceived as a complementary activity in organizations so that they can dedicate themselves to their primary business (Gorla & Somers, 2014).

Barile et al. (2020) report that service transactions are evolving, and the emerging nature has increased complexity and uncertainty, becoming increasingly unpredictable in the business environment. However, researchers are concerned about the innovation gap in service research, pointing out as significant factors lean investment in research and development initiatives (Gallouj & Djellal, 2011; Rajapathirana & Hui, 2018), and by less technological and dynamic feature, when compared to the industry (Kubota, 2006).

Studies analyzing innovation in services have been growing at a slow pace. One of the motivations is based on traditional innovation research, which promotes new technologies and tangible artefacts, while the service sector rarely formalizes R&D initiatives or produces them (Gallouj & Djellal, 2011).

Risk scenarios can be enhanced and accelerated in processes and business models in the services segment, including leading companies to suffer an interruption of activities, incurring high costs, and facing the possibility of litigation in disagreement with the service sector's existence, as a solution to problems for customers (Gadrey, Gallouj & Weinstein, 1995; Mcleod & Dolezel, 2018).

3 Methodological Procedures

Bibliometrics was used to investigate publications on the subject. The qualitative approach made it possible to examine and measure the publications and their particularities to provide more significant support for analyzing the generated results.

The descriptive analysis (Gil, 2002) considered a quantitative survey of publications. At this stage, the evolution of the number of articles published per year was explored to identify the trend of interest in the theme "cybernetic risks in the service sector" in the literature of business management without disregarding the existing content in other areas of research. Cybernetics is an interdisciplinary field, based on existing knowledge (Kim, 2004; Kandjani et al., 2012), and the service sector is perceived as plural, intangible, and shareable (Fitzsimmons & Fitzsimmons, 2014).

Furthermore, this study used the method of organization and systematization of information presented by Chueke & Amatucci (2015), whose structure followed the premises of the Bradford, Lotka, and Zipf laws, using the scientific databases of the Web of Science of CAPES platform, as shown in Table 2:

Table 2

Bibliometric laws

Author	Law	Focus	Description	
Samuel C. Bradford	Bradford's Law	Periodicals	$A(r) = a + b.\log (r)$	A(r) = cumulative number of articles on the same subject published by different journals r = cumulative *ranking* a and b = constants
Alfred J. Lotka	Lotka 's Law	Authors	$Y = C/X^2$	X = number of publications Y = number of authors with x publications C = constant
George K. Zipf	Zipf 's Law	Words	$f(n) = K/n$	f(n) = frequency of occurrences of a word n = order of frequency K = constant

Source: Guedes & Borschiver (2015); Chueke & Amatucci (2015)

Bradford's Law can be applied to identify the most prominent scientific journals which published studies on cyber risks in services. Analyzing the distribution of scientific articles on this topic in different journals makes it possible to identify which publications have stood out and which provide a solid base of knowledge.

Lotka's Law can be used to investigate the productivity of authors, identifying those who are prolific and their respective contributions. This analysis not only helps to understand the perspectives and approaches taken in the field of cyber risk in the service sector but also assists in identifying authors whose research may be relevant to the study.

And lastly, applying Zipf's Law in analyzing studies on cyber risks in services allows for exploring the distribution of the most frequent keywords found in the scientific literature. Analyzing the frequency of these terms makes it possible to obtain clarity about the main risks, threats, and even mitigating actions that permeate business models.

This analysis seeks a reasoned direction for study, allowing more precise identification of knowledge gaps that deserve more attention. Additionally, this study will use tools such as the VOSviewer to broaden this analysis. By visualizing research data, the VOSviewer allows us to identify connections and patterns among the most recurrent terms and themes in the literature, contributing to the understanding of the field of study of cyber risks in services.

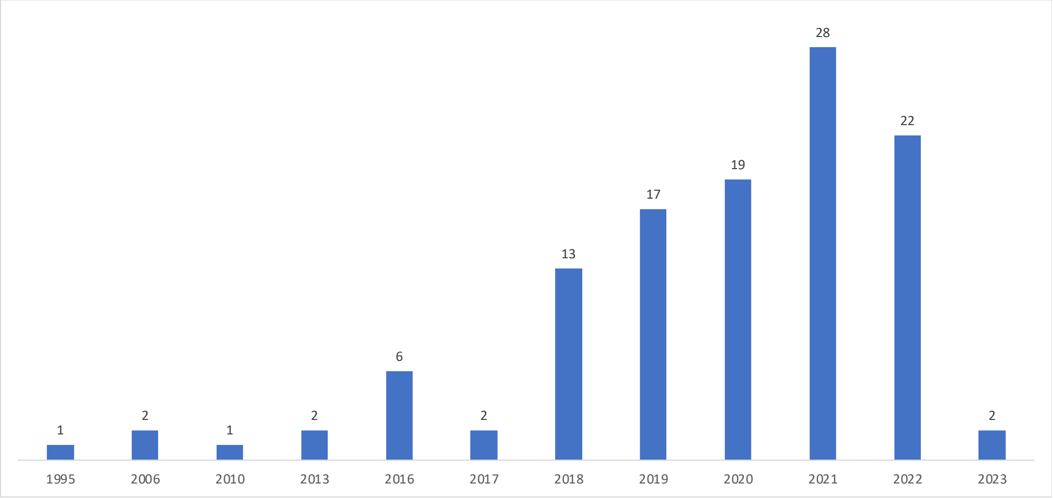
4 Presentation and Analysis of Results

Bibliometrics was applied to identify, collect, and analyze the relevant data in the scientific literature related to cyber risks in services. With the purpose of analyzing the characteristics of publications on the theme, the methodology first proceeded to collect data using the terms "cyber risks" and "services*" without any temporal cut-off. Using the scientific databases of the Web of Science (WoS), it was decided to search the publications by "topic" to achieve the functionality of searching for occurrences in the terms indicated by the title, abstract, and keywords brought by the authors.

In the article selection process, a key criterion focused on the relevance of the content concerning the research question was adopted. The objective was to select articles that directly addressed the theme in question and established a relationship, even if indirect, with the objective and the question outlined for this research. By applying this criterion, we sought to ensure the inclusion of the most pertinent studies, contributing to the quality and validity of the research. The exclusion criteria adopted considered articles that did not focus on the research objective and those that were not peer-reviewed. Studies covering cyber risks in services increased significantly in the last five years, as can be seen in in Graph 1.

Graph 1

Annual scientific production on Cyber Risks on Services



Source: Research Data

The results allowed collecting publications from December 1995 to February 2023, reaching 624. After analyzing these publications, a new filter was applied, restricting the search. As a result, 115 articles were obtained with a focus on the research theme and were peer-reviewed.

The results show that the topic has grown in importance, with the increase in publications from 2018 onwards. It is possible to identify a gap since 1995, in which the first article on the topic advocated the "banks of tomorrow", pointing out the opportunities and risks of the digital banking environment.

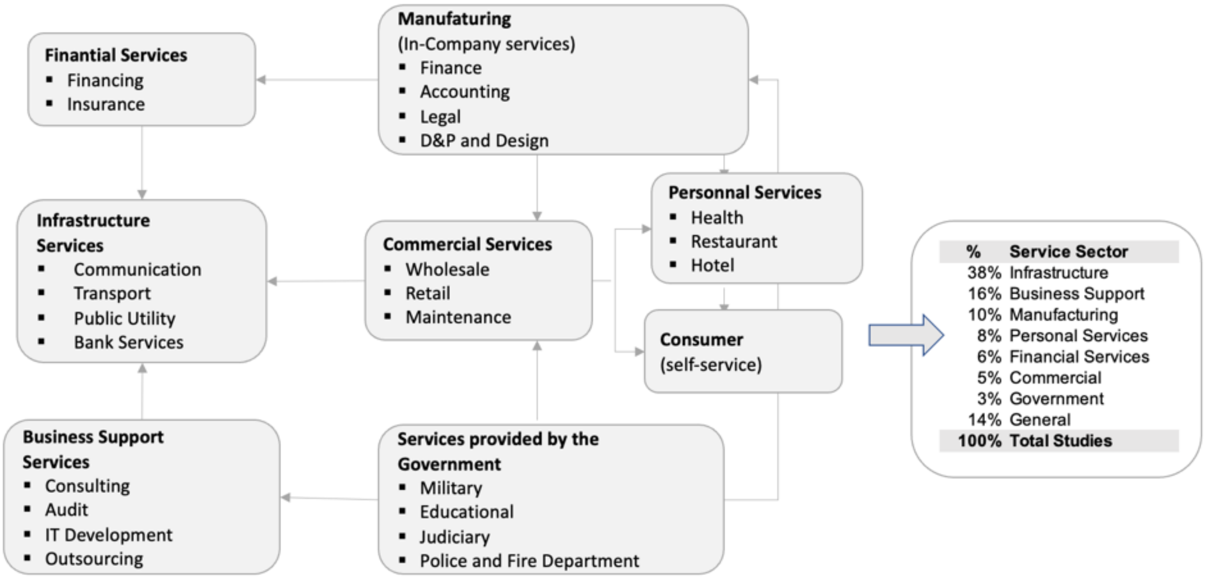
4.1 Organization of Scientific Publications by Research Area and Service Sector

In the WoS - Web of Science database, publications were grouped according to the research area and the sector of the service area to which the studies were directed. Initially, the publications were organized into ten areas, with the following order of publication relevance: Computer Science and Information Systems (58%), Engineering (35%), Business, Finance, and Management (29%), Telecommunications (26 %) and, Methods of Theory of Computer Science, Artificial Intelligence of Computer Science (these last three with 5%).

When exploring the scientific production of cyber risks in the service sector, we sought to identify in which sectors the studies focused on the theme. The exploration included reading and analyzing the 115 articles, allowing their classification according to service sectors. In addition, they were quantified and observed, starting from the model proposed by Fitzsimmons & Fitzsimmons (2014), as shown in Figure 1.

Figure 1

Cyber risks in the Services sector



Source: Adapted from Fitzsimmons & Fitzsimmons (2014).

In the analysis, studies around infrastructure (38%) stood out, which can be justified by the functionality of the complex economy that makes up these types of services, which act as a means of distribution for customers, constituting an essential sector for the industry (Fitzsimmons & Fitzsimmons, 2014).

Knowledge-Intensive Business Services (KIBS) are business services and operations heavily dependent on professional knowledge, commonly recognized as business support services. The statistic

(16%) presented for these types of services remains in line with the finding of Desmarchelier, Djellal, and Gallouj (2013), who claim that the source of increased labor productivity shifted from industry to services, even though the motor of the outsourcing process continues to be the industrial sectors, dependent on KIBS.

In sequence, there is the area of manufacturing services (10%), consisting of decision-making and internal controls of companies. It was considered essential to highlight the item “General” (14%), composed of studies that address the service sector, however, in a generic way, such as the Internet of Things, case studies and discussions on cybersecurity. By identifying the research areas with the highest concentration of the proposed theme, the results obtained can open the opportunity to deeply evaluate other sectors of the service area, such as the personal, commercial, and financial sectors.

Regarding government action, the opportunity may lie in coercive measures and legal consequences to deal with cyber-crimes committed against companies and individuals. In this regard, Mcleod and Dolezel (2018) understand that federal laws should impose heavy penalties for facilities whose negligence contributes to data breaches.

4.2 Most Used Key Expressions

Following the criteria of Zipf's Law, after reviewing the literature, the most recurrent key expressions that favor the search for the theme of "Cyber Risks" and "Services," used together for almost three decades were obtained. However, these expressions also came to contribute to other search results.

After analyzing the 624 articles, which resulted in 115 for this study, we used VOSviewer to enhance the visualization of the information. When loading the text files extracted from WoS into VOSviewer, it was chosen to use the functionality "Create a map based on text data". Then the "Title and abstract fields" option was chosen in the "Choose files" field to include the title and abstract fields in the analysis. In the "Choose counting method" section, "Binary counting" was selected as the counting method. The binary count assigns the value of "Occurrences" to the number of documents in which a term occurs at least once, and a minimum occurrences threshold of 5 was set in the "Minimum number of occurrences of a term" field under the "Choose threshold." These procedures extended Zipf's Law criteria, allowing better visualization of the key expressions in VOSviewer. With the resulting map, we obtained a more explicit and comprehensive representation of the main themes and interconnections in the analyzed articles.

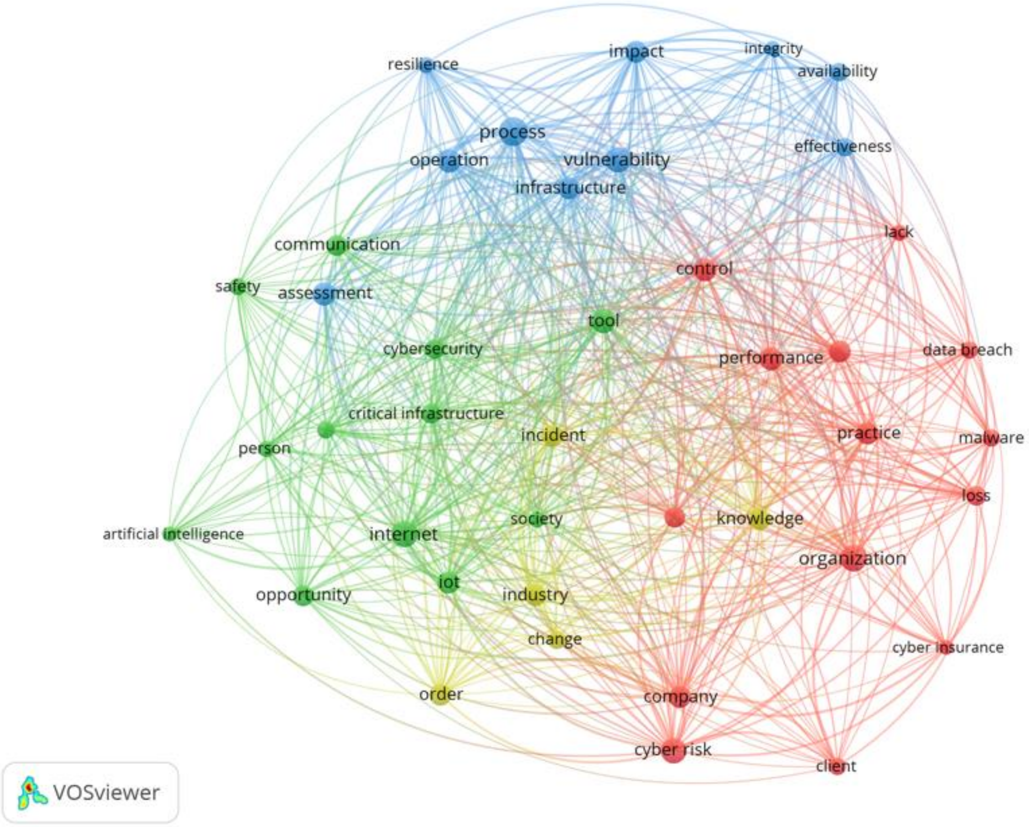
In the calculation, keywords were identified by the WoS to represent the articles of the research theme. The most frequent word is "process", obtained 37 times, followed by the terms "internet" 36, and "vulnerability" 33 times. In addition, terms that do not have a specific concept adhering to the research theme were identified and discarded, words such as "study," "case," and "publication."

To better understand the interaction of the critical expressions obtained by the clusters that highlighted points of analysis alluding to cyber risks in the service sector, Figure 2 presents the terms obtained by the visualization technique of the density of citations through each point (cluster).

Each point in the item density view has a corresponding color, which indicates the density of the items at that point. By default, in the visualization, the relationship between the colors and the distance of keywords indicates that the closer they are together, the stronger the relationship between them. The size of the image represented in the cluster demonstrates its density, whereas the larger circle reflects the representativeness of the item in the sample (Van Eck & Waltman, 2020).

Figure 2

Network Analysis



Source: Research Data / VOSviewer 1.6.19

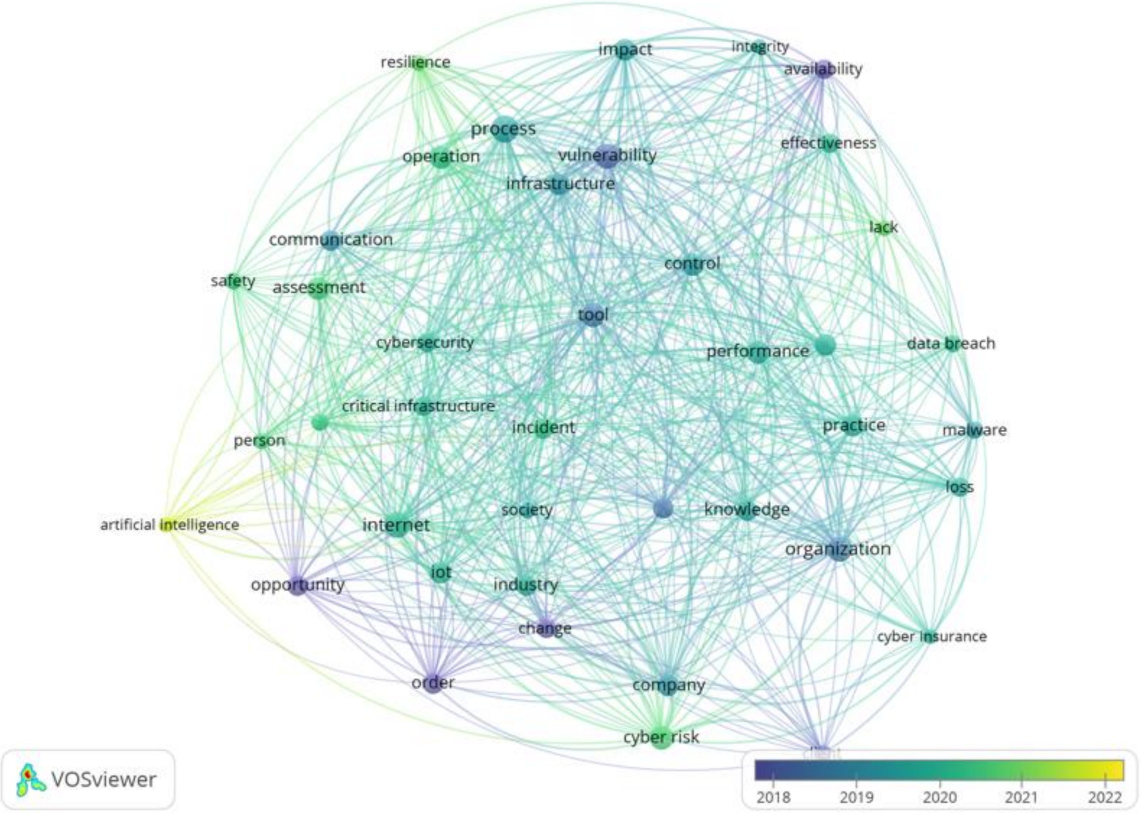
In figure 2, the red cluster conglomerates terms linked to mitigating factors that can characterize threats in the cybernetic environment, such as activities and control performance, knowledge, and cybersecurity that permeate an organization's processes, whether by identifying attacks, violations of data, losses (financial, operational and reputational) or lack of knowledge.

Next, the blue cluster (figure 2) represents the studies dedicated to understanding cyber risk using the Internet of Things. The terms "vulnerability" and "infrastructure" stand out, in which the literature highlights attacks, damage, and subtraction of user information. Terms such as assessment, effectiveness, integrity, and resilience represent actions to face risks related to future and uncertain events, requiring a more profound knowledge of the processes to manage them.

While the green cluster highlights the Internet of Things (IoT) and Artificial Intelligence as elements inserted in the cybernetic risk literature, the scenario brought by the green cluster is, in a way, absorbed by the red cluster, highlighting factors such as incidents, change, knowledge, industry and consequently, orders (purchases).In the researched literature, terms such as critical infrastructure, communication, and security are also highlighted, linked to the information of customers (company or individual) who carry out their technological transactions on the Internet. It is necessary to consider the relevance of threats and risks in recent years, starting in 2018, with the increase in publications related to recent discussion topics, as shown in Graph 1 and Figure 3.

Figure 3

Recent Discussion Topics



Source: Research Data / VOSviewer 1.6.19

In Figure 3, analyzing the topics discussed from 2018 onwards, by the blue cluster, terms such as vulnerability, tool, availability, change, and opportunity demonstrate the concern with cyber risks at the organizational infrastructure as researchers began to turn their attention to these terms from that period onwards, as shown in Graph 1.

The yellow cluster represents more recent studies covering service companies concerning artificial intelligence, a field of knowledge that has been studied and applied to the service sectors, private or public, essential for the functioning of society and the economy, which confirms the statistics obtained in this research area (Figure 1).

After exposing the types of publications, in addition to the most frequent and recent keywords related to cyber risks in the service sector, the analysis of scientific production was increased to identify the primary sources of impact, authors and the most relevant articles and collaboration in research between countries on this topic.

4.3 Most Cited Articles

Applying Lotka's Law (Chueke & Amatucci, 2015), Table 3 shows the most cited publications on Cyber Risk in the Services Sector. The most cited articles were published in the last five years, reinforcing the relevance of scientific dissemination in the face of threats and attacks that companies and individuals have faced. However, the sample may be tiny, given the financial and economic relevance brought by cyber risks and attacks that occurred globally.

Table 3

The most cited articles

No. Quotes	Title	Authors	Periodical	Year
239	Relationship between innovation capability, innovation type, and firm performance	Rajapathirana, RP Jayani; Hui, Yan	Journal of Innovation & Knowledge	2018
143	A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services	Stellios, Ioannis; Kotzanikolaou, Panayiotis Psarakis , Mihalis; Alcaraz , Cristina; Lopez, Javier	IEEE Communications Surveys and tutorials	2018
90	TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems	Alsaedi, Abdullah; Mustafa, Nour; Tari, Zahir; Mahmood, Abdun; Anwar, Adnan	IEEE Access	2020
86	Cybersecurity in Distributed Power Systems	Li, Zhiyi; Shahidehpour, Mohammad; Aminifar, Farrokh	Proceedings of the IEEE	2017
75	Adaptive Formation of Microgrids with Mobile Emergency Resources for Critical Service Restoration in Extreme Conditions	Che, Liang; Shahidehpour, Mohammad	IEEE Transactions Power Systems	2019
72	Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach	Ullah, Farhan; Naeem, Hamad; Jabbar, Sohail; Khalid, Shehzad; Latif, Muhammad Ahsan; Al- Turjman, Fadi; Mostarda, Leonardo	IEEE Access	2019
51	Data security and consumer trust in FinTech innovation in Germany	Stewart, Harrison; Juerjens, Jan	Information Computer Security	2018
55	A Survey of Moving Target Defenses for Network Security	Sengupta, Sailik; Chowdhary, Ankur; Sabur, Abdulhakim; Alshamrani, Adel; Huang, Dijiang; Kambhampati, Subbarao	IEEE Communications Surveys and tutorials	2020
40	Cyber-analytics: Modeling factors associated with healthcare data breaches	McLeod, Alexander; Dolezel, Diane	Decision Support Systems	2018

Source: Research Data.

When considering the importance of the most cited articles in the scientific community, it is essential to strike a balance between the recognition and validity of the study. The articles analyzed (Table 3) converge in recognizing cyber risks and the importance of implementing adequate security measures. The authors highlight the need to protect organizations and users from cyber threats to preserve systems' confidentiality, integrity, and availability. In addition, three articles focus on the risks associated with the Internet of Things (IoT), addressing the challenges faced in critical infrastructure and home environments. The services sector is identified as an area of concern, emphasizing sectors such as insurance, FinTech, and power distribution.

While sharing associations, the papers differ regarding specific contexts and proposed approaches. Each one addresses a particular context, such as innovation in insurance companies, IoT security, cybersecurity in distributed electrical systems, threat detection in IoT, consumer confidence in FinTech, and data breach analysis in healthcare. This diversity of contexts reflects the breadth of industries in which cyber risks are relevant. In addition, the papers present distinct approaches to address cybersecurity challenges. This includes using intrusion detection systems, moving target defense, deep learning techniques, and adaptive security measures. These different approaches highlight the need for a comprehensive and adaptive approach to fight the ever-evolving cyber threats.

The remaining articles from the survey, not listed in Table 3, address the importance of cybersecurity in specific sectors, such as healthcare, banking, e-commerce, and the oil and gas and infrastructure, demonstrating a concern about protecting sensitive data and systems in these areas due to the risks associated with potential security breaches. In addition, there are discussions about using cyber insurance to manage risk, indicating organizations' recognition of the need to protect against damage from cyber incidents. Another highlight is the Internet of Things (IoT), mentioned in several articles, which brings security challenges due to the increasing interconnectivity of devices and systems - this expands the attack surface and underscores the importance of adequately addressing cyber risks in the context of IoT. Additionally, common discussion points are the detection and prevention of cyber-attacks such as botnets, ransomware, and command-and-control traffic, highlighting the need for effective mechanisms to defend and protect against evolving threats.

An interesting feature to emphasize in these ten most cited articles is that at least seven are signed by more than four authors, reaching eight in a single article. What can be inferred from this sample is the fact that the topic of cyber risks in the service sector brings together a more significant number of researchers due to the complexity and multiplicity of topics.

It is also clear that IEEE Xplore stands out from other journals in terms of scientific and technical publications centered on computer science and electronics. However, risk management also involves other areas of knowledge, such as administration, economics, and sociology.

4.4 Most Cited Authors

Using the premises of Lotka's Law (Chueke & Amatucci, 2015), the most relevant authors of the data sample obtained were identified. Among them, the ten most cited authors are shown in Table 4, followed by the quantity of the respective citations and the number of published articles.

Table 4

Most cited authors

Author	Number of citations	No. Publications
Rajapathirana, RPJ	239	1
Hui, Y.	239	1
Shahidehpour, M	161	2
Stellios, I.	144	2
Kotzanikolaou, P	144	2
Psarakis, M	143	1
Alcaraz, C	143	1
Lopez, J.	143	1
Li, Z.	86	1
Che, L	75	1

Source: Research Data.

With the results shown in Table 4, researchers have recently worked on the topic that covers cyber risks in the service sector, considering that the sample showed an average of one publication for the ten most cited authors.

Although the article "Relationship between innovation capability, innovation type, and firm performance" by authors Rajapathirana & Hui (2018) received significant prominence via citations, this article does not explore cyber risks in services in detail - it only highlights that cyber risks are a relevant concern for the industry concerning innovation capability and performance of insurance firms.

The other authors' research areas are linked to the challenges and threats encountered in the cyber environment and the services provided in this context. Ioannis Stellios focuses on Information Security, covering topics such as encryption, intrusion detection, and protection of confidential information. Panayiotis Kotzanikolaou focuses his analysis on Privacy, Encryption, and Critical Infrastructures. Mihalis Psarakis explores Trusted Embedded Systems and Integrated Circuit Testing, seeking to secure systems in medical devices, automobiles, and industrial equipment. Cristina Alcaraz focuses on the Internet of Things (IoT) and IT Security. Javier Lopez focuses on IT Security broadly, addressing topics such as cryptography, network security, and defense strategies. Zhiyi Li research Power System Operations, Cybersecurity, and Smart Cities. Finally, Liang Che focuses on Power System Operations and Control. It was possible to obtain the authors' respective research areas through WoS (Web of Science), complementing the information obtained in the bibliometric study. The list of the most cited authors can help guide researchers who wish to explore the cyber risk and services theme.

4.5 Publications by Countries

By identifying the origin of articles published in a given research area, it is possible to obtain a view of the geographic distribution of scientific production and identify the countries or institutions leaders in cyber risks in the service sector. Researchers from the United States have been leading the volume of publications, followed by the United Kingdom, Netherlands, Switzerland, and, in fifth position, Mexico. Also, Table 5 shows the countries with the highest publications in the investigated databases.

Table 5

Publications by Countries

Position	Countries	Number of publications
1	United States	43
2	United Kingdom	22
3	Netherlands, Switzerland	13
4	Germany	6
5	Mexico	3
7	Spain, Japan, Romania, and Ukraine	4
8	China, Colombia, Croatia, France, India, South Korea, Poland	3

Source: Research Data.

It is important to highlight that the set of 115 analyzed works was published in 17 countries by researchers from 47 different nationalities - which can demonstrate the decentralized and pulverized form in which the theme of cybernetic risks in services is found. However, due to the plurality of countries and researchers, it is inferred that the subject has become a global concern, even with the scarcity of publications.

The Cryptocurrency Crime Report, issued by ChainAnalisys (2021), revealed the ranking of countries that have received the highest volumes of cryptocurrencies from illicit addresses based on the analysis of the locations of service users. Among the first five positions in this assessment are the United States and the United Kingdom, which may justify the leadership of these countries in publications related to cyber risks in the service sector.

5 Discussion

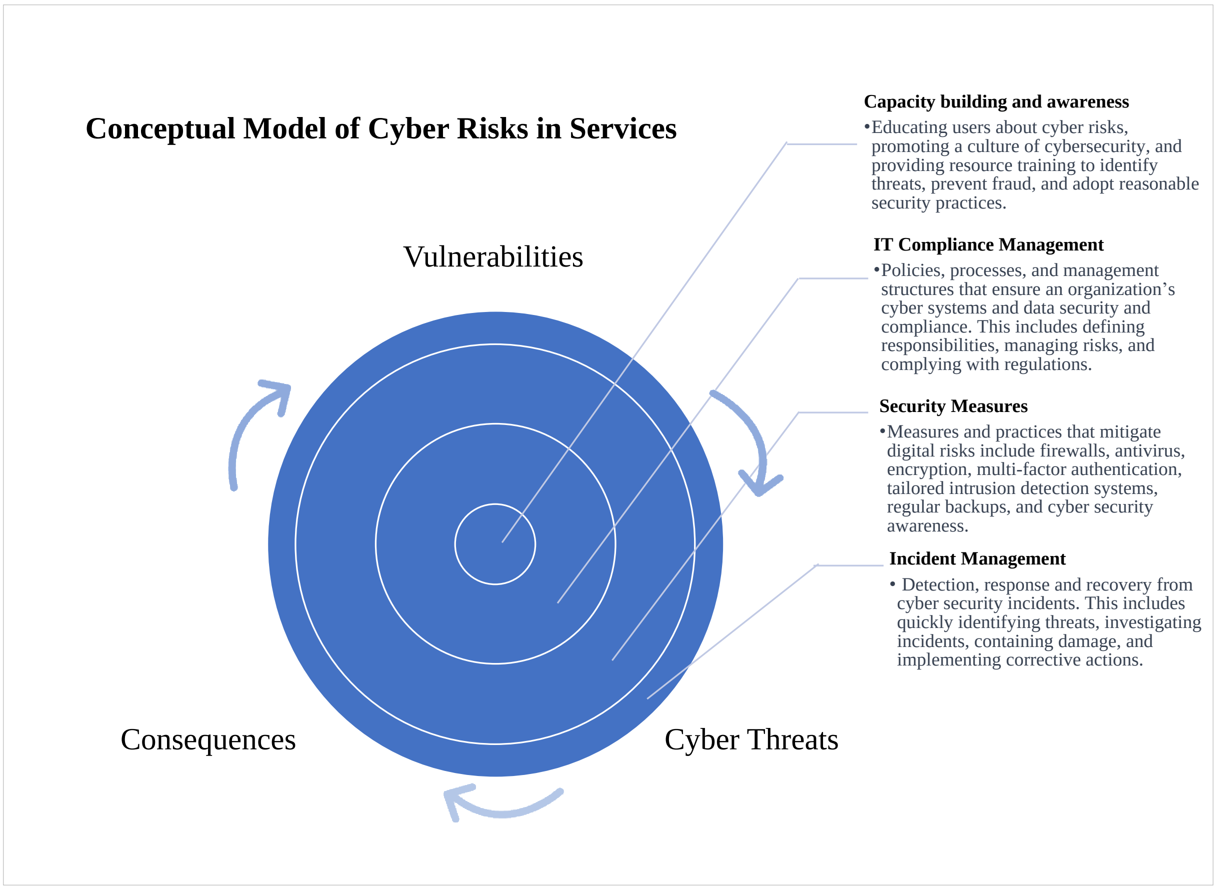
The 115 identified publications have in common a focus on cyber risks and information security in different contexts. Although each addresses specific aspects, most recognize the importance of addressing cyber risks to protect assets, ensure customer trust, and promote innovation. In addition, most articles mention the Internet of Things (IoT) as a field where cyber risks are especially relevant. They point out that IoT devices in critical infrastructure and home environments can be entry points for cyber-attacks, requiring appropriate security measures to protect data privacy and ensure system integrity.

The involvement and importance of services sectors in the economy encompass infrastructure, intensive business services in knowledge, manufacturing, and other sectors, as indicated in Figure 1. These sectors provide essential services to society and are interconnected with others, playing a pivotal role in economic development. However, the publications reinforce the understanding that the services sector also faces cyber risks that can compromise efficiency, security, and reliability and negatively affect the business operations of customers, suppliers, and the government. The publications are virtually unanimous that adopting security measures and risk management strategies would strengthen the resilience of these sectors and ensure the continuity of services provided.

One gap identified after reviewing the publications is the lack of models or guidelines that consider cyber risks across different subsectors of the service sector, such as financial services, healthcare, tourism, retail, and others. Based on the published work, a conceptual model was developed as a starting point for addressing the emerging demands of the service sector. This model provides a comprehensive framework (Figure 4) that effectively addresses the challenges faced to date while striving to meet the needs identified in the trend line. It can even be extended to other sectors of the economy beyond the services sector.

Figure 4

Conceptual Model of Cyber Risks in Services



Conceptual Model of Cyber Risks in Services

Capacity building and awareness

- Educating users about cyber risks, promoting a culture of cybersecurity, and providing resource training to identify threats, prevent fraud, and adopt reasonable security practices.

IT Compliance Management

- Policies, processes, and management structures that ensure an organization’s cyber systems and data security and compliance. This includes defining responsibilities, managing risks, and complying with regulations.

Security Measures

- Measures and practices that mitigate digital risks include firewalls, antivirus, encryption, multi-factor authentication, tailored intrusion detection systems, regular backups, and cyber security awareness.

Incident Management

- Detection, response and recovery from cyber security incidents. This includes quickly identifying threats, investigating incidents, containing damage, and implementing corrective actions.

Source: Elaborated by authors (2023)

This model proposes adopting a cyclical, continuous improvement approach to address these three elements: vulnerabilities, cyber threats, and consequences. This involves identifying and assessing existing vulnerabilities, developing and implementing appropriate security measures to mitigate the identified threats, and constantly monitoring threats and consequences to adjust and improve security practices continuously.

Capacity building and awareness: this model proposes capacity building and cyber risk awareness at the core of cyber risk mitigation in the service sector. Based on the assumption that enabling and training stakeholders (in addition to employees, customers, and suppliers) is critical to strengthening a company's resilience to uncertainty and risk, training is aligned to develop relevant skills, adapt to change, better use resources (systems and policies), and make decisions. From the works reviewed in this study, examples include challenges related to e-commerce technology and business that require knowledge-driven coping by users (Liu et al., 2022), knowledge development and training for cybercrime investigators (Johnson et al., 2020), as well as training for machine learning models, IoT security, and network traffic classification (Guan et al., 2021).

Additionally, coupling capacity building with compliance in IT management, Sipior et al. (2021) expound applying a "real world" case study to provide recommendations related to the IT operational risks of an organization in its operations, financial reporting, and compliance.

IT Compliance Management: Defining responsibilities through investments in cyber insurance to transfer some of the risks associated with potential breaches in the future (Bodin et al., 2018). Also, Rifat et al., 2019, highlighted the importance of cyber risk management and ensuring compliance and quality of e-services (taxes) in e-government. Additionally, compliance in IT management includes leaders involved in transitional support, focused on improving governance and integration, and transformational support, which involves fostering a new cultural mindset for cyber resilience (Loonam et al., 2022).

Security Measures: cybersecurity plays a relevant part in the service sector. Implementing security measures such as using advanced technologies and forming microgrids (Li et al., 2017; Che & Shahidehpour, 2019) can help mitigate risks and ensure service continuity in disasters or cyber-attacks. Consumer trust and service quality are essential factors in adopting innovations, such as the financial technologies (Stewart & Jurjens, 2018). The articles highlight the need to invest in robust cybersecurity measures and high-quality services to gain customer trust and promote wider adoption of technological innovations - such as cloud computing which has gained buy-in from businesses due to its scalability, stability, and high availability (Ouedraogo & Mouratidis, 2013; Akinrolabu et al., 2019; Torkura et al., 2020).

Incident Management: regarding incident management, publications also emphasize the need for innovative and adaptive approaches to cybersecurity, such as using intrusion detection systems adapted for Industrial Internet of Things (IIoT) applications and Moving Target Defense (MTD)[3]. These approaches aim to mitigate cyber risks by overcoming attackers' advantages and continuously adapting to attacks (Bruger et al., 2019; Alsaedi et al., 2020; Sengupta et al., 2020).

The literature review and the bibliometric study allowed us to deepen the content analysis of the publications in a way that could bring a model that not only represents and communicates the concepts and relationships that involve cyber risk+s in the service sector but that makes them more accessible, allowing a better understanding of the theme for the development of future research.

6 Final Remarks

By combining these two themes, cyber risks, and the service sector, it was possible to address the specific challenges that arise when transacting through e-commerce and the threats to the confidentiality and integrity of information. In addition, device security is also included, which involves

[3] The central goal of MTD is to create a dynamic computing environment where key system elements such as IP addresses, network ports, protocols, and configurations are constantly changed or masked.

the risks associated with network-connected devices, whose publications have extensively discussed IoT.

Many services currently rely on IoT devices to operate efficiently in the service sector. For example, in healthcare, energy, and transportation industries, IoT plays a crucial role in monitoring and controlling critical systems. Service companies can take appropriate security measures to protect their systems and infrastructure from potential attacks by understanding the cyber risks associated with IoT devices. This may involve implementing robust security practices such as strong authentication, data encryption, and continuous monitoring of IoT devices.

In addition, publications have addressed concerns about the infrastructure environment, where cyber risks are associated with the security and operation of critical infrastructure systems such as power grids, transportation, water, healthcare, telecommunications, and other critical facilities. This covers the vulnerabilities of these devices and a fraud-prone environment. This is because services developed in the cyber environment involve processing and storing sensitive information, such as users' personal and financial data, making them potential targets for cyber-attacks.

The timid number of publications may indicate that the topic of cyber risks has not received attention from researchers in nearly 30 years. This may result from lower awareness of cyber risks in earlier periods or a lack of academic interest in exploring the subject. The presence of many authors on a topic with few publications suggests that cyber risk research involves an interdisciplinary approach. This is because cyber risk is a complex area that encompasses technical, legal, ethical, social, and behavioral aspects. Therefore, the collaboration of diverse experts may be necessary to understand the challenges associated with this topic entirely.

Nevertheless, another point that contributes to this perspective that the theme of cyber risks is not widely discussed or referenced in the scientific literature is the number of citations. This may result from insufficient conceptual development, research, or a less consolidated theoretical base. Considering the increasing relevance of cyber security, it can be inferred that cyber risks should draw more attention from researchers. With the rapid evolution of technology and growing cyber threats, there is an increasing need to explore and understand these risks in depth.

This study adopted as a criterion for elaborating the sample analyzed in the bibliometric study the publications that contained the keywords "cyber risks" and "services*" mentioned in the topic item in the WoS. In this research, prominent publications were presented that can be explored in depth by researchers in the service sector, especially cyber risks in the sectors highlighted in Figure 1, which can be an interesting opportunity to expand empirical research considering the plurality of the theme of services and considering that the greater the connectivity, the greater the company's subjection to cyber risks.

The literature review conducted in this study ratified the scientific value of bibliometric studies and the contributions to the field, considering that:

(i) The research revealed the potential for exploring the topic, in which the areas of services and their representativeness in research related to cyber risks were identified.

(ii) It enabled the conceptual organization of cyber risks and its core/focus of understanding (Table 1).

(iii) Can identify emerging trends and clusters in service sector activities (Fig. 2 and 3).

(iv) Development of the conceptual model (Fig. 4) aims to be an initial framework, providing input for future research and ongoing development in the services sector.

The findings are considered relevant for researchers who wish to delve into a particular service activity in addition to other sectors of the economy. Moreover, this study sought to arouse the interest of researchers from different areas, such as administration, technology, and sociology, going beyond theoretical frameworks and focusing on application and operationalization in the organizational context.

References

Abbagnano, N. (2007). *Dicionário de Filosofia*, São Paulo: Martins Fontes.

Amanowicz, M., & Kamola, M. (2022). *Building Security Awareness of Interdependent Services, Business Processes, and Systems in Cyberspac*e. Electronics, 11(22), 3835.

Brazil Agency. (2020). *Serviços avançam e comércio cai como parcela do PIB desde 1947*. Retrieved on february 01, 2023, from https://agenciabrasil.ebc.com.br/economia/noticia/2020-12/servicos-avancam-e-comercio-recua-na-participacao-no-pib-desde-1947 .

Barile, S., Grimaldi, M., Loia, F., & Sirianni, CA (2020). Technology, value Co-Creation and innovation in service ecosystems: Toward sustainable Co-Innovation. *Sustainability*, 12(7), 2759.

Biener, C., Eling, M., & Wirfs, JH (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1), 131-158.

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527-544.

Böhme, R., Laube, S., Riek, M. (2018). A fundamental approach to cyber risk analysis. *Variance*, 12 (2), 161–185.

Brewer, D. (2000). *Risk assessment models and evolving approaches.* IAAC Work. Retrieved January 29, 2023, from www.gammassl.co.uk/research/archives/events/IAAC.php .

Cebula, JL, & Young, LR (2010). *A taxonomy of operational cyber security risks.* Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Chain Analysis (2021). *The 2021 Crypto Crime Report – Everything you need to know about ransomware, darknet markets, and more.* Retrieved January 28, 2023, from https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf .

Chueke, GV., & Amatucci, M. (2015). O que é bibliometria? Uma introdução ao Fórum. *Internext*, *10*(2), 1-5.

Conger, S., Pratt, JH., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal, 23*(5), 401-417.

Desmarchelier, B., Djellal, F., & Gallouj, F. (2013). *Knowledge intensive business services and long term growth.* Structural Change and Economic Dynamics, 25, 188-205.

Durak, T. (2020). Innovation spaces: the new campus risk paradigm. In Challenges *for Health and Safety in Higher Education and Research Organizations*, pp. 304-336. Royal Society of Chemistry.

Egan, R., Cartagena, S., Mohamed, R., Gosrani, V., Grewal, J., Acaryya, M., ... & Ang, K. (2019). Cyber operational risk scenarios for insurance companies. *British Actuarial Journal,* 24.

Fang, E., Palmatier, RW, & Steenkamp, JBE (2008). Effect of service transition strategies on firm value. *Journal of Marketing,* 72(5), 1-14.

Fitzsimmons, JA, & Fitzsimmons, MJ (2014). *Service Administration: Operations, Strategy and Information Technology.* Amgh Publisher.

Funke, Martha. (2021). Empresas lançam soluções voltadas para riscos cibernéticos. *Jornal Valor.* Consultado em 28 de janeiro de 2023, em https://valor.globo.com/publicacoes/suplementos/noticia/2021/03/25/empresas-lancam-solucoes-voltadas-a-riscos-ciberneticos.ghtml

Gadrey, J., Gallouj, F., & Weinstein, O. (1995). New modes of innovation: how services benefit industry. International Journal of Service Industry Management.

Gallouj, C. (1997). Asymmetry of information and the service relationship: selection and evaluation of the service provider. International Journal of Service Industry Management.

Gallouj, C. (2023). Information Economy, Knowledge Economy, Intangible and New Economy... What Next? In F. Gallouj, C. Gallouj, M. C. Monnoyer, & L. Rubalcaba (Eds.), Elgar Encyclopedia of Services (pp. 119-121). Edward Elgar Publishing.

Gallouj, F., & Djellal, F. (Eds.). (2011). The handbook of innovation and services: a multi-disciplinary perspective. Edward Elgar Publishing.

Ghorbani, HR, & Ahmadzadegan, MH (2017, November). Security challenges in internet of things: survey. In *2017 IEEE Conference on Wireless Sensors* (ICWiSe), 1-6. IEEE.

Gil, AC (2002). *Como elaborar projetos de pesquisa,* vol. 4, p. 175. São Paulo: Atlas.

Gorla, N., & Somers, TM (2014). The impact of IT outsourcing on information systems success. *Information & Management,* 51(3), 320-335.

Guan, J., Cai, J., Bai, H., & You, I. (2021). Deep transfer learning-based network traffic classification for scarce dataset in 5G IoT systems. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3351-3365.

Guedes, V. L., & Borschiver, S. (2005). Bibliometria: uma ferramenta estatística para a gestão da informação e do conhecimento, em sistemas de informação, de comunicação e de avaliação científica e tecnológica. *Encontro nacional de ciência da informação*, *6*(1), 18.

ISO/IEC (2014). *ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary.* International Organization for

Standardization/International Electrotechnical Commission (ISO/IEC). Retrieved January 28, 2023, from https://www.iso.org/standard/63411.html

Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts. *The Journal of Criminal Law*, *84*(5), 427-450.

Kandjani, H., Wen, L., & Bernus, P. (2012). Enterprise architecture cybernetics for collaborative networks: Reducing the structural complexity and transaction cost via virtual brokerage. *IFAC Proceedings*, 45(6), pp. 1233-1239.

Kim, J. H. (2004). Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural. *Horizontes antropológicos*, *10*, 199-219.

Klimburg, A. (Ed.). (2012). *National cyber security framework manual.* NATO Cooperative Cyber Defense Center of Excellence.

Kubota, LC. (2006). Inovação tecnológica das empresas de serviços no Brasil. *In* JA Negri, LC Kubota (Orgs.). *Estrutura e dinâmica do setor de serviços no Brasil.* Indivíduo. 2. Instituto de Pesquisa Econômica Aplicada. Brasília: IPEA, 35-72.

Lévy, P. (2000). *Cibercultura.* 2ª ed. São Paulo: Editora 34.

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce, Front. Psychol., 19 October 2022, Sec. Organizational Psychology.

Mantha, B. R., & García de Soto, B. (2021). Assessment of the cybersecurity vulnerability of construction networks. *Engineering, Construction and Architectural Management*, *28*(10), 3078-3105.

Melo, H. P. D., Rocha, F., Ferraz, G. T., Di Sabbato, A., & Dweck, R. H. (1998). *O setor serviços no Brasil: uma visão global*-1985/95.

McAfee (2021). *What is malware*? Retrieved January 28, 2023, from https://www.mcafee.com/en-us/antivirus/malware.html

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57-68.

Metters, R. (2023). Service Operations. In F. Gallouj, C. Gallouj, M. C. Monnoyer, & L. Rubalcaba (Eds.), *Elgar Encyclopedia of Services* (pp. 183-185). Edward Elgar Publishing.

Mittal, B. (1999). The advertising of services: meeting the challenge of intangibility. *Journal of Service Research*, *2*(1), 98-116.

NAIC (2018). Cybersecurity Risk Management. *National Association of Insurance Commissioners (NAIC)*. Retrieved January 30, 2023, from https://content.naic.org/consumer/cybersecurity.htm.

Neghina, DE, & Scarlat, E. (2012). Managing information technology security in the context of cyber crime trends. *International journal of computers communications & control*, 8(1), 97-104.

Nieuwesteeg, B., Visscher, L., & de Waard, B. (2018). The law and economics of cyber insurance contracts: a case study. *European Review of Private Law*, 26(3).

NIST - National Institute of Standards and Technology (2006). Minimum security requirements for federal information and information systems, Federal Information Processing Standards Publication FIPS PUB 200. National Institute of Standards and Technology (NIST), Gaithersburg, MD. Retrieved January 30, 2023, from https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf .

Nordin, F., Kindström, D., Kowalkowski, C., & Rehme, J. (2011). The risks of providing services: Differential risk effects of the service-development strategies of customisation, bundling, and range. *Journal of Service Management*, *22*(3), 390-408.

Nonaka, I., o Nonaka, I., Ikujiro, N., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation* (Vol. 105). OUP USA.

Pal, R., Huang, Z., Lototsky, S., Yin, X., Liu, M., Crowcroft, J., ... & Nag, B. (2021). Will catastrophic cyber-risk aggregation thrive in the IoT age? A Cautionary Economics Tale for (Re-)Insurers and Likes. *ACM Transactions on Management Information Systems* (TMIS), 12(2), 1-36.

Powers, M. R. (2006). Pure vs speculative risk: False choice; sham marriage. *The Journal of Risk Finance*, *7*(4), 345-347.

Raddats, C., Kowalkowski, C., Benedettini, O., Burton, J., & Gebauer, H. (2019). Servitization: A contemporary thematic review of four major research streams. *Industrial Marketing Management*, *83*, 207-223.

Rajapathirana, RJ, & Hui, Y. (2018). Relationship between innovation capability, innovation type, and firm performance. *Journal of Innovation & Knowledge*, 3(1), 44-55.

Rifat, A., Nisha, N., & Iqbal, M. (2019). Predicting e-tax service adoption: Integrating perceived risk, service quality and TAM. *Journal of Electronic Commerce in Organizations* (JECO), 17(3), 71-100.

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review*, 31(3), 701-728.

Rubalcaba, L., & Solano, E. (2023). Services Economic Growth. In F. Gallouj, C. Gallouj, M. C. Monnoyer, & L. Rubalcaba (Eds.), *Elgar Encyclopedia of Services* (pp.92-94). Edward Elgar Publishing.

Saraiva, J. (2021). *Novos hábitos fazem gastos com entrega crescerem 149% em 2020* . Jornal valor. suplementos. Consultado em 28 de janeiro de 2023, em https://valor.globo.com/publicacoes/suplementos/noticia/2021/06/29/novos-habitos-fazem-gastos-com-entregas-crescerem-149-em-2020. ghtml .

Saridakis, G., Benson, V., Ezingeard, JN, & Tennakoon, H. (2016). Individual security information, user behavior and cyber victimization: An empirical study of social networking users. *Technological Forecasting and Social Change*, 102, 320-330.

Silva, W. R., & Nogueira, J. M. (2019). Ataques cibernéticos e medidas governamentais para combatê-los. *O Comunicante*, *9*(1), 42-57.

Sipior, J. C., Lombardi, D. R., & Gabryelczyk, R. (2021). Information Technology Operational Risk: A Teaching Case. *Journal of Computer Information Systems*, *61*(4), 328-344.

Stoshikj, M., Kryvinska, N., & Strauss, C. (2016). Service systems and service innovation: two pillars of service science. *Procedia computer science*, *83*, 212-220.

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, 135, 105143.

United Nations Conference (2017). *The role of the services economy and trade in structural transformation and inclusive development.* Trade and Development Board. Geneva, July 2017. Retrieved January 28, 2023, from https://unctad.org/system/files/official-document/c1mem4d14_en.pdf .

Van Eck, NJ, Waltman, L. (2020). *VOSviewer Manual: Manual for VOSviewer version 1.6.17* . 25 November 2020. Universiteit Leiden/ CWTS. Retrieved January 28, 2023, from https://www.vosviewer.com/documentation/Manual_VOSviewer_1.6.16.pdf.

Wiener, N. (1984). *Cibernética e sociedade: o uso humano de seres humanos.* São Paulo: Cultrix, 1984.

Wiener, N. (2017). *Cibernética ou controle e comunicação no animal e na máquina* . Tradução de Gita K. Guinsburgl. 1st ed. São Paulo: Perspective

World Economic Forum. (2012). *Global risks 2012.* Seventh edition, Insight Report, Geneva.

Younan, M., Houssein, EH, & Ali, AA (2020). Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement*, v. 151.

Zeithaml, VA (2017). *Excelência em atendimento.* Saraiva Educação SA.