Cuadernos de Turismo, nº 53, (2024); pp. 243-260
eISSN: 1989-4635
DOI: https://doi.org/10.6018/turismo.616471

Universidad de Murcia

CYBERSECURITY IN TOURISM AND HOSPITALITY MANAGEMENT RESEARCH: CURRENT ISSUES, TRENDS, AND AN AGENDA FOR FUTURE RESEARCH

*Maria del Mar Alonso-Almeida**
Universidad Autónoma de Madrid
https://orcid.org/0000-0003-4957-3689
*Carlo Giglio***
University of Calabria
https://orcid.org/0000-0001-7244-1049

ABSTRACT

This paper compares two literature reviews on cybersecurity issues focused on the mature organisations, business and management field, and the embryonic tourism and hospitality area. Hence, we use the general study on the former as a benchmark for the narrower review on the latter, to map the current trends and identify the corresponding gaps. Findings suggest the following topic clusters for future research: (1) machine learning, artificial intelligence, blockchain, big data; (2) fraud and reputation; (3) phishing and social engineering; (4) human security and user education.

Keywords: Cybersecurity; cybercrime; cyberattack; cyber education.

Fecha de recepción: 7 de marzo de 2024.
Fecha de aceptación: 19 de abril de 2024.

* Facultad de Ciencias Económicas y Empresariales. Departamento de Organización de Empresas. Ciudad Universitaria de Cantoblanco. 28049 MADRID (España). E-mail: mar.alonso@uam.es
** Department of Mechanical, Energy and Management Engineering; RENDE (Italy).
School of Economics, Business and Accounting, University of São Paulo; SÃO PAULO (Brazil).
University of Science and Technology of China, HEFEI CITY (China). E-mail: carlo.giglio@unical.it

Ciberseguridad en la investigación en turismo y hotelería: temas de actualidad, tendencias y una agenda para futuras investigaciones

RESUMEN

Este artículo compara dos revisiones bibliográficas sobre cuestiones de ciberseguridad centradas en el ámbito de las empresas y la gestión empresarial, por una parte, y en el sector del turismo y la hostelería por otra. De este modo, se utiliza el estudio general en el ámbito empresarial como punto de referencia para el análisis sobre el sector del turismo, con el fin de trazar las tendencias actuales e identificar las lagunas existentes. Los resultados sugieren los siguientes temas para futuras investigaciones: (1) aprendizaje automático, inteligencia artificial, blockchain y big data; (2) fraude y reputación; (3) phishing e ingeniería social; (4) seguridad y educación.

Palabras clave: Ciberseguridad; ciberdelito; ciberataque; educación cibernética.

1. INTRODUCTION

Digitalisation has transformed the tourism sector with radical changes in operational, value chain, and relationship with tourists in the two last decades (Sigala, 2018). The tourism industry has adopted technological innovations such as internet infrastructure, diverse payment systems, point-of-sale (POS), and IoT and Blockchain (Chen and Fiscus, 2018). Nevertheless, this revolution is not without its challenges. Nowadays, one of riskiest challenges in tourism is the occurrence of cyberattacks due to the increase of cybercrime (Boto-Garcia, 2023). In fact, tourism was reported as one of more attacked industries in recent years (Security, 2023).

Some of the reasons making the tourism industry vulnerable to cybercrime are, on the one hand, the growth of technology adoption in the industry, the ubiquity of IT infrastructure, a lack of IT security culture, and the high rate of new or low skilled employees (Gwebu and Barrows, 2020).

On the other hand, the tourism industry accumulates valuable personal and financial information on its customers (Parsons *et al*., 2021). This kind of information can be used by cybercriminals, not only to extort money from companies in the sector, but also to attack individual customers. These data breaches are aggravated when dealing with particularly sensitive data such as health data in medical tourism (Parsons *et al*., 2021). In addition, to build a cybersecurity capability, cybersecurity in companies was tackled from a technology and compliance-oriented approach instead of a business-driven approach (Paraskevas, 2022).

The types of cyberattacks mostly reported by the industry are phishing and malware attacks, especially POS attacks and ransomware that have provoked direct and indirect losses (Paraskevas, 2022). Some authors emphasize that this problem differs between tourism and non-tourism companies in terms of actors, actions, assets, and attributes (Gwebu and Barrows, 2020).

Although, health, bank, and government industries have been highly attacked, tourism has also been victim of cybercrime. Companies such as Marriot, Starbucks, Hilton, Pizza Hut and McDonald's, among others, have reported different types of breaches (Bilefsky, 2017; Chen and Fiscus, 2018; Gwebu and Barrows, 2020) and this threat is increasing.

Thus, cybersecurity is a hot emerging topic in tourism. However, very little research has addressed this issue (Chen and Fiscus, 2018) despite the impacts associated with these security breaches (Butler, 2016; Paraskevas, 2022). In fact, most of the previous research about cybersecurity in tourism is descriptive. One part of the research has focused on analysing the type of breaches, identifying the source of risks and providing some recommendations (Chen and Fiscus, 2018; Gwebu and Barrows, 2020; Parsons *et al*., 2021). Another part has developed theoretical models to develop a cybersecurity environment (Roy, 2021; Laso *et al*., 2022; Paraskevas, 2022; Sahu and Gutub, 2022). Empirical research is, however, residual (Boto-Garcia, 2023).

Therefore, this study attempts to respond to an existing gap in tourism research regarding the status of cybersecurity and its impact on the tourism industry and identify priority research directions. In the following sections, the methodology of the study is explained, the results are presented and, finally, the discussion and conclusions are disclosed.

2. METHODOLOGY

Building on the multi-step approach for systematic literature reviews (Denyer and Tranfield, 2009), we have: 1) made the review questions explicit; 2) defined the review scope; 3) identified, checked, and selected the publications that proved to be relevant to the reviews; and 4) read and synthesised their contents (see also Giglio *et al*., 2023a). The compared systematic literature reviews have been conducted by adopting the PRISMA methodology (Page *et al*., 2021; Moher *et al*., 2009). We adopted the comparison among two different literature reviews in order to use the more mature field related to organizations, business and management as a benchmarking tool for forecasting the future research directions and topic clusters within the embryonic literature on cybersecurity in tourism and hospitality. We used the following search strings in Scopus on 18 September, 2023 to select the relevant articles. In detail, we have identified and searched for the relevant keywords in titles, abstracts, and keyword sections of each article.

For the systematic literature review on cybersecurity in tourism and hospitality, we have used the following search string: (KEY (*cyberatt**) OR KEY (*cybersecurit**) OR KEY (*cybercrime**)) AND (KEY (*tourism*) OR KEY (*hospitality*) OR KEY (*travel*) OR KEY (*travel* AND *agenc**) OR KEY (*restaurants*)). For the systematic literature review on cybersercurity in organisation, business, and management fields, we have used the following search string: (KEY (*organization** OR *business** OR *management*) AND (KEY (*cyberatt**) OR KEY (*cybersecurit**) OR KEY (*cybercrime**))) AND (LIMIT-TO (SRCTYPE,"*j*")) AND (LIMIT-TO (DOCTYPE,"*ar*") OR LIMIT-TO (DOCTYPE,"*re*")) AND (LIMIT-TO (SUBJAREA,"*BUSI*") OR LIMIT-TO (SUBJAREA,"*SOCI*") OR LIMIT-TO (SUBJAREA,"*ECON*") OR LIMIT-TO (SUBJAREA,"*DECI*")) AND (LIMIT-TO (LANGUAGE,"*English*")).

For the former, we obtained an initial set of 18 papers, whilst we identified 453 articles for the latter systematic review. Our search results were double checked to ensure that there is no overlapping among the sets related to tourism and hospitality and to organisations, business and management. This was also possible due to the selection of two ad hoc sets of different keywords for each specific literature review, and to the more stringent use of the "AND" logical operator while combining keywords. Moreover, the searches were not extended to title and abstract, in order to make the results more coherent with the objectives of the two reviews.

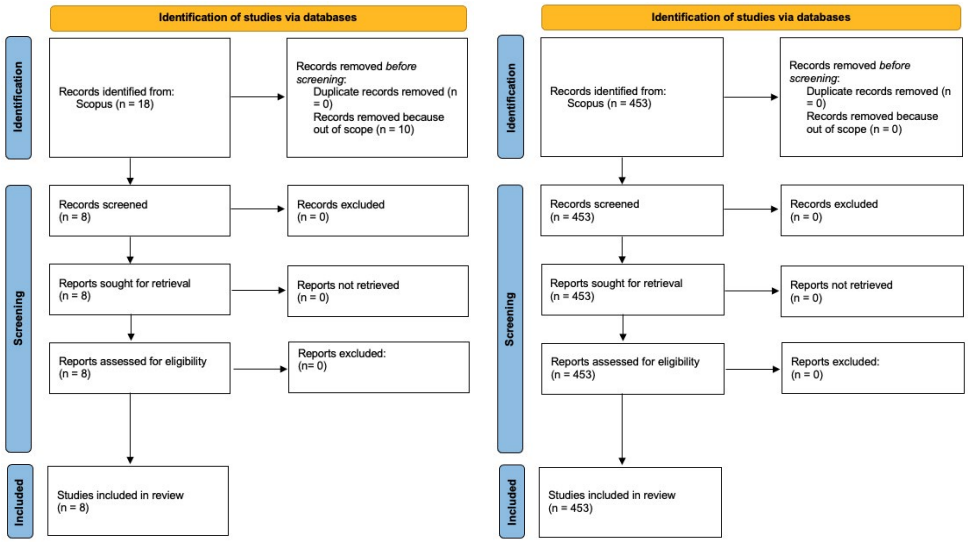
The selection of Scopus was motivated by Franceschini *et al*. (2016) that showed how the use of Web of Science - or other more stringent databases - would have limited the number of analyzed articles, especially for the smaller dataset on tourism and hospitality (see also Schiederig *et al*., 2012). On the other side, Google Scholar includes more publications than Scopus or Web of Science. However, it is proven to be an excellent source for literature discovery, but it embraces all kinds of publications (e.g., reports, working papers, conference proceedings, student theses/assignments, etc.) (Bornmann *et al*., 2008, Delgado López-Cózar *et al*., 2014, Giustini and Kamel Boulos, 2013, Lasda Bergman, 2012), finally, indexing a "*significant mass of non-refereed web documents which do not pass any 'qualitative' process*" (Kousha and Thelwall, 2007, p. 290).

We report the results of the PRISMA methodology for the new systematic reviews in Figure 1, adapted from the updated PRISMA 2020 flow diagram (Page *et al*., 2021; Moher *et al*., 2009; see also Giglio *et al*., 2023a). The diagrams consist in four steps, from identification of potentially relevant publications, to screening including an eligibility check, and inclusion. Specifically, for each set of articles, we have analysed the abstract of each article, checked for duplicates, and verified the relevance and appropriateness of the articles with respect to the scope of the corresponding review (Page *et al*., 2021; Moher *et al*., 2009). We have not imposed constraints on Scopus subject areas, language, and article type for the review on tourism and hospitality, given the already reduced amount of publications (18) existing in Scopus – besides, the selected publications fall within the same subject areas and language as the second set of articles. In fact, we have removed ten out-of-scope contributions from the review on cybersecurity in tourism and hospitality, while no changes were made to the other set of articles, based on inclusion/exclusion criteria in Table 1 (Page *et al*., 2021; Moher *et al*., 2009). Finally, we have considered 8 articles for the review of cybersecurity in tourism and hospitality and 453 for cybersecurity in the organisation, business, and management fields. The description of the characteristics of the final samples is reported in Table 2.

A mixed, quali-quantitative approach has been adopted at this stage. In fact, the following step consisted of a qualitative analysis of the full papers, which was performed in parallel by all the authors (Giglio *et al*., 2023a; Giglio *et al*., 2023b). On completion of the analysis, all the authors shared all their evaluations with one another in order to provide the highest transparency and to make sure that they could explore and integrate all the findings and contributions of each article in a flexible manner (Kraus *et al*., 2022; Giglio *et al*., 2023a; Zahoor *et al*., 2020). In further detail, all full papers were investigated and coded by all authors until a shared consensus was obtained (Pittaway *et al*., 2004). Then, the two sets of full papers were also analysed quantitatively by using the R-Studio

software app Biblioshiny (Aria and Cuccurullo, 2017; Giglio *et al*., 2023a; Giglio *et al*., 2023b). In this second step, we have deepened the authors' productivity, citations, and impacts as well as the relevance of publication sources, the evolution of topics over time, and the emerging trends in terms of keywords and thematics (Aria and Cuccurullo, 2017; Giglio *et al*., 2023a; Giglio *et al*., 2023b).

Figure 1
A COMPARISON OF THE PRISMA FLOW DIAGRAMS FOR SYSTEMATIC REVIEW ON CYBERSECURITY IN TOURISM AND HOSPITALITY (LEFT SIDE) AND IN ORGANISATION, BUSINESS AND MANAGEMENT (RIGHT SIDE)



Source: Authors own elaboration.

Table 1
INCLUSION AND EXCLUSION CRITERIA

Review of cybersecurity in tourism and hospitality		
Criteria code	**Inclusion criteria**	**Exclusion criteria**
1	Articles dealing with cybersecurity	Articles not dealing with "Inclusion criteria 1"
2	Articles dealing with tourism and hospitality at large including travel and restaurants	Articles not dealing with "Inclusion criteria 2"

Review on cybersecurity in organisation, business, and management fields		
Criteria code	**Inclusion criteria**	**Exclusion criteria**
3	Articles dealing with cybersecurity	Articles not dealing with "Inclusion criteria 3"
4	Articles dealing with tourism and hospitality at large including travel and restaurants	Articles not dealing with "Inclusion criteria 4"
5	Articles in Scopus subject areas related to Business-Management-Accounting, Economics-Econometrics-Finance, Decision Sciences, Social Sciences	Articles not included in Scopus subject areas "Inclusion Criteria 5"
6	Articles (including reviews) published in journals	Articles not published in journals
7	Articles written in English	Articles not written in English

Source: Authors own elaboration.

Table 2
DESCRIPTIONS OF THE TWO DATASETS OF ARTICLES ON TOURISM AND HOSPITALITY AND ON ORGANISATION, BUSINESS AND MANAGEMENT

Review of cybersecurity in tourism and hospitality	
Description	**Results**
Timespan	2018:2023
Sources (Journals, Books, etc)	7
Documents	8
Annual Growth Rate %	0
Document Average Age	1.75
Average citations per doc	5.125
References	246
Author's Keywords (DE)	32
Authors	20
Authors of single-authored docs	3
Single-authored docs	3
Co-Authors per Doc	2.5
International co-authorships %	37.5
Article	6

Book chapter	1
Conference paper	1
Review of cybersecurity in organisation, business and management	
Description	**Results**
Timespan	2003:2023
Sources (Journals, Books, etc)	208
Documents	453
Annual Growth Rate %	26.61
Document average age	2.79
Average citations per doc	11.85
References	24255
Author's keywords (DE)	1675
Authors	1227
Authors of single-authored docs	77
Single-authored docs	85
Co-authors per doc	3.01
International co-authorships %	21.85
Article	419
Review	34

Source: Authors own elaboration.

3. RESULTS

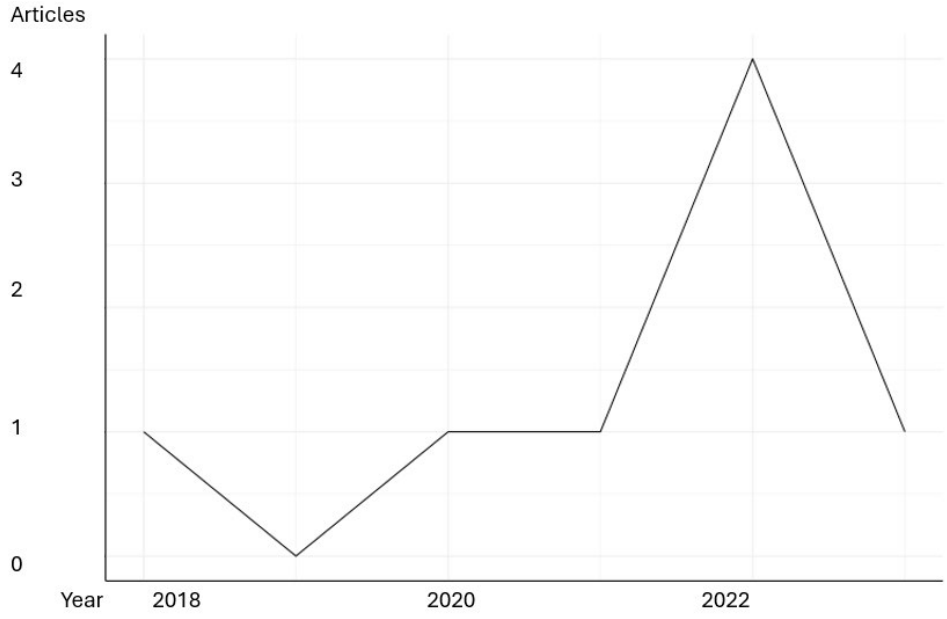
The analysis of the different aspects for both reviews took into consideration author-related factors (e.g. productivity, citations, and impacts), source-related dimensions (e.g. relevance of publication sources), trends of topics and keywords, thematic evolution of topics over time, co-occurrence network, and factorial analysis about topics and keywords. Figures 2 and 3, and Figures 4 and 5, show the yearly rate of scientific productivity related to the articles analysed for each review and the citations trends per article and per year, respectively.

All 8 articles for the review on tourism and hospitality have been published in the last lustrum, from 2018 to 2023, highlighting the recency of the general topic and the timeliness of the review as well as a poorer interest in the topic over the previous decades, compared to the general organization, business and management fields. By contrast, the review on cybersecurity in organisation, business, and management identified 453 articles in the last two decades, namely, from 2003 to 2023. Whilst for the latter review, we have found a consolidated growth trend of publications, predominantly from 2016 (Figure 3), up to a maximum of 112 in 2023, the former review on tourism and hospi-

tality shows a fluctuating trend of published articles (Figure 2) that demonstrates the underdeveloped discourse in the field literature and the lack of structured and systematised knowledge about cybersecurity issues. This fact is even more telling if we consider that the annual scientific productivity is not related to the single author in the field (i.e., it is not a per capita productivity), but it represents an absolute value of the overall community working on such topics. Hence, the difference in absolute values returns the magnitude in terms of the delay of the literature discourse in tourism and hospitality compared to the general field of organisations, business and management: the former is 56 times less investigated than the latter. This has further shown the inevitable need for a literature discourse in this field to be driven and oriented depending on the development of the more developed and consolidated literature on cybersecurity in organisation, business, and management, which is taken as a reference in this comparison study.

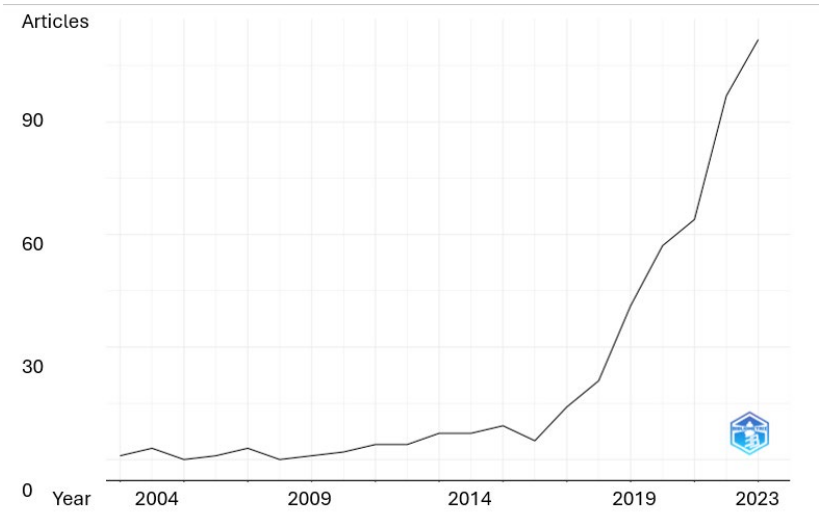
The fluctuating trend of yearly citations in the tourism and hospitality review (Figure 4), is coherent with the fluctuations of the corresponding scientific productivity (Figure 2) of up to a maximum of 4 in 2022. On the contrary, the maximum average citations per article and per year that grew to 51.21 and 7.32, respectively, was reached in 2017, whilst the turbulent growth of publications reached its peak in 2023 with 112 articles (Figure 3), so far.

Figure 2
ANNUAL SCIENTIFIC PRODUCTIVITY FOR THE REVIEW ON CYBERSECURITY IN TOURISM AND HOSPITALITY



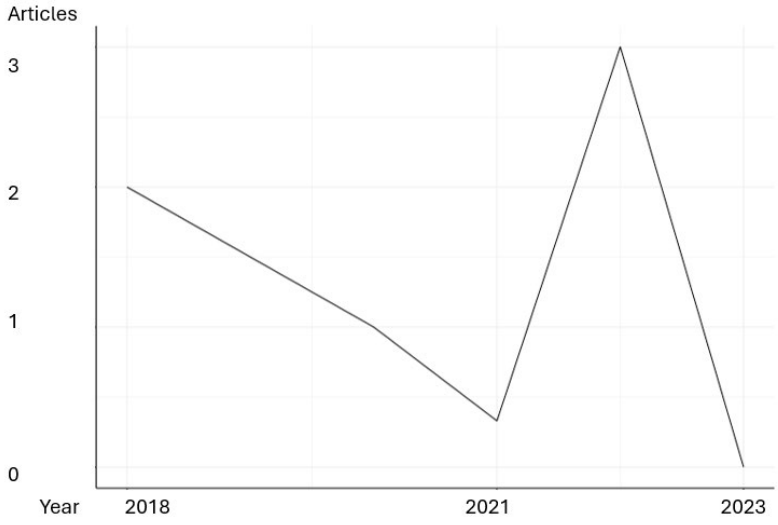
Source: Authors own elaboration.

Figure 3
ANNUAL SCIENTIFIC PRODUCTIVITY FOR THE REVIEW ON CYBERSECURITY IN ORGANISATION, BUSINESS, AND MANAGEMENT



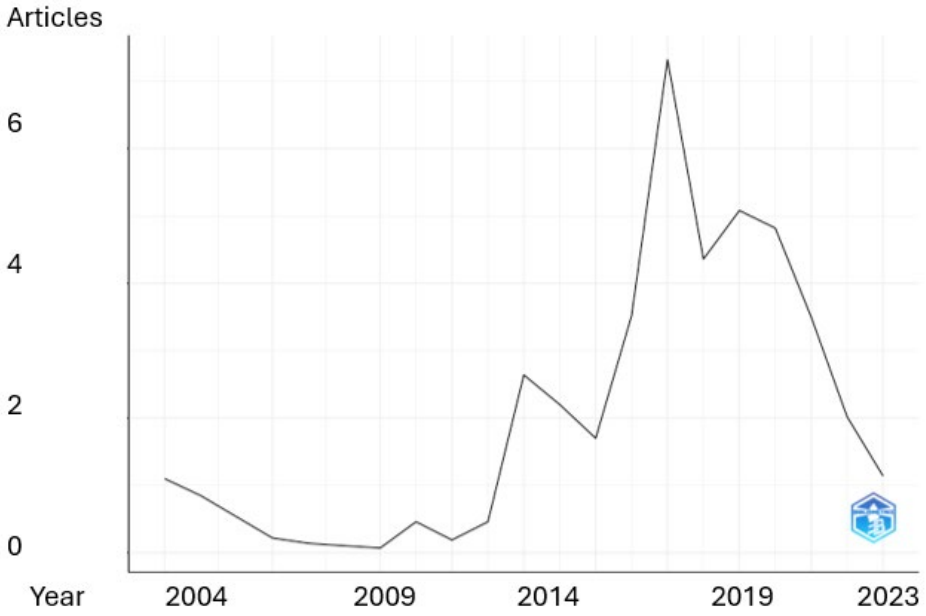
Source: Authors own elaboration.

Figure 4
ANNUAL CITATIONS PER ARTICLE FOR THE REVIEW ON CYBERSECURITY IN TOURISM AND HOSPITALITY



Source: Authors own elaboration.

Figure 5
ANNUAL CITATIONS PER ARTICLE FOR THE REVIEW ON CYBERSECURITY IN ORGANISATION, BUSINESS, AND MANAGEMENT



Source: Authors own elaboration.

The peppered production for cybersecurity in tourism and hospitality is reflected by the authors' production over time that shows just 1 publication per author, whilst a more intensified and continued effort characterises the authors in the field of organisation, business, and management, up to 6-7 publications in a row. Likewise, the maximum number of articles per most relevant author is equal to 1 for tourism and hospitality, whilst it is equal to 7 for organisation, business, and management, with more than 1 article for more than 100 authors, thus, suggesting that the scientific leadership in terms of authors' productivity is quite dispersed.

As for the sources of publication, the most frequent sources in the dataset are predominantly non-top-ranked outlets (e.g., Journal of Hospitality and Tourism Technology and Handbook of E-Tourism), thus, suggesting that cybersecurity has not yet been recognised as a key issue in the ongoing discourse in tourism and hospitality, whilst some key journals are included among the most relevant sources in organisation, business, and management (e.g., IEEE Transactions on Engineering Management, Business Horizons). This is confirmed by the homogeneity in source ranking based on the Bradford's Law - which ranks the publication sources and articles through the source log (rank) – according to which most of the journals retrieved as core sources in the more general dataset outperforms the

tourism and hospitality ones. Interestingly, the analysis of publication sources suggests that most of the outlets publish technology-related articles but tend to neglect social and behavioural aspects like those related to social engineering issues, human security and user education in the tourism and hospitality fields.

Moreover, the analysis of the disciplinary contents of each publication has been conducted by considering the authors' keywords as the main and more reliable source to understand the inner meaning and contribution of each article (Giglio *et al.,* 2023a; Giglio *et al.,* 2023b). Afterwards, we have also deepened the themes and topics emerging from the two sets of articles. More precisely, Figure 6 shows that the ongoing discourse on cybersecurity in tourism and hospitality has not taken very differentiated research directions as it remains anchored at the predominant keywords that are typical of very general cybersecurity issues (i.e. cyberattacks, cybercrimes, privacy, risk and data breach, and similar topics) except for themes linked to cruises and crew members. Thus, this again confirms the need for a driven development of the literature discourse based on a by-analogy comparison with the organisation, business, and management research fields. On the other side, cybersecurity in organisation, business, and management is characterised by a richer and more differentiated development of the literature (Figure 7), which embraces risk-related topics, artificial intelligence, Internet of Things, blockchain, Industry 4.0, Covid-19, digitalisation, resilience, knowledge management, and supply chain management. The comparison among the two word clouds in Figures 6 and 7 shows that there is a delayed pattern of differentiation of the topic clusters within the narrower review on tourism and hospitality, whilst the larger one on organization, business and management clearly identifies trends and clusters related to technology-driven research (e.g., Industry 4.0, artificial intelligence, machine learning, big data), social security aspects (e.g., social engineering risks), behavioural and educational research (e.g., user education and training), trust and reputation (e.g., frauds, digital payments). Therefore, we use this review, which is endowed with more advanced literature on cybersecurity in the general organisation, business, and management area, in order to forecast the delayed literature discourse in the tourism and hospitality industry and provide tourism and industry stakeholders with future research directions. First, Figure 8 shows that after focusing on more general topics linked to cybersecurity, research on organisation, business, and management has emphasised themes related to artificial intelligence and blockchain, Industry 4.0, and digitalisation, which are the emerging topics depicted by the thematic evolution shown in Figure 9. In conclusion, the advanced thematic evolution of organisation, business, and management research could help in predicting that future research directions and applications in tourism and hospitality will be more heavily focused on the hitherto emerging clusters in the following: (1) machine learning, artificial intelligence, blockchain, and big data; (2) fraud and reputation in the assurance and banking sectors that could be applied to digital payment methods and transactions in general in tourism and hospitality; (3) phishing and social engineering related to data breach and privacy issues in tourism and hospitality; and (4) human security and user education applied to tourism and hospitality crew and customers, not limited to the sector of cruises.

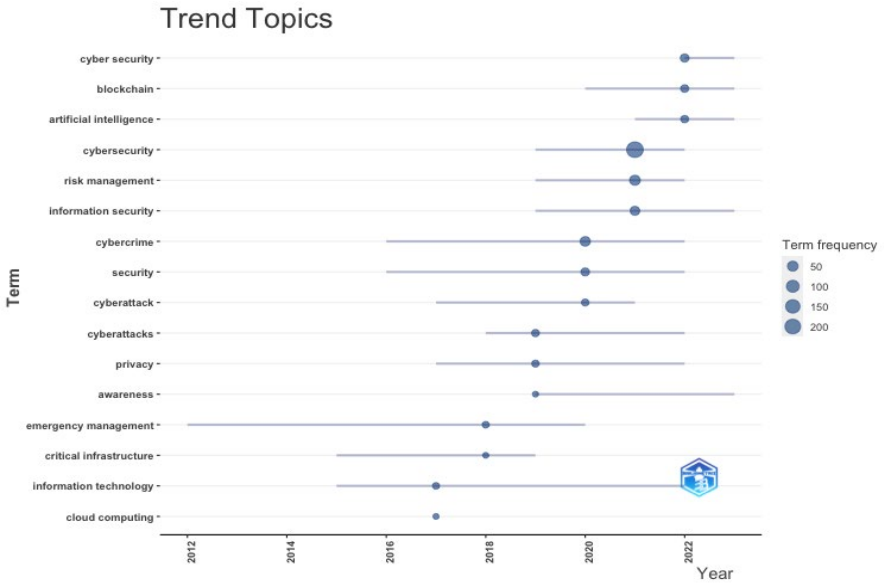
Figure 6
WORD CLOUD FOR THE REVIEW ON CYBERSECURITY IN TOURISM AND HOSPITALITY

Source: Authors own elaboration.

Figure 7
WORD CLOUD FOR THE REVIEW ON CYBERSECURITY IN ORGANISATION, BUSINESS AND MANAGEMENT

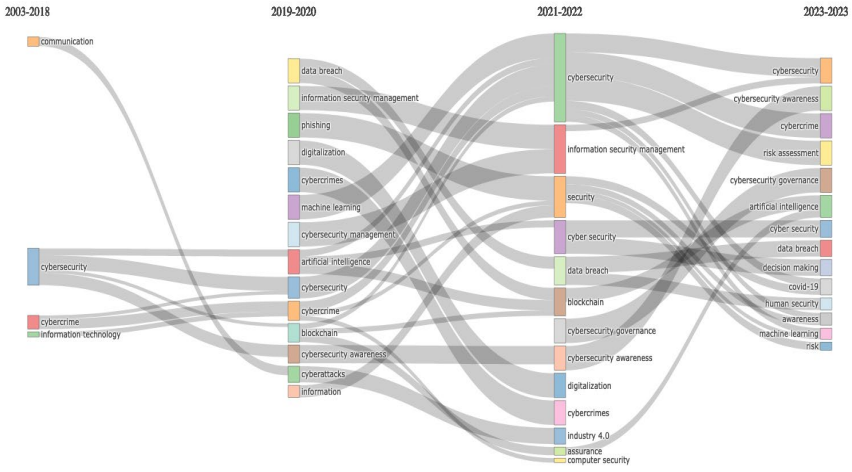
Source: Authors own elaboration.

Figure 8
TREND TOPICS FOR THE REVIEW ON CYBERSECURITY IN ORGANISATION, BUSINESS, AND MANAGEMENT



Source: Authors own elaboration.

Figure 9
THEMATIC EVOLUTION FOR THE REVIEW ON CYBERSECURITY IN ORGANISATION, BUSINESS, AND MANAGEMENT



Source: Authors own elaboration.

4. DISCUSSION AND CONCLUSIONS

Lohrke and Frownfelter-Lohrke (2023) analysed articles published from 1998 through to 2022 in the Financial Times (FT) 50 journals in order to identify the topics in cybersecurity that scholars have examined across different business disciplines. A total final sample of 150 articles was identified in management research. 47% of the research was published in the period 2017-2022. The authors found that cybersecurity has been analysed across four major perspectives: antecedents of, reactions to, and outcomes from cybersecurity threats, and potential moderators of this process. Management approach, accounting, marketing, operations, and ethics have been the most used frameworks to study cybersecurity issues. Regarding management theories risk assessment, protection motivation and governance are the most frequently employed theories with very little attention to other management theories. Thus, these authors provide future opportunities for management research on cybersecurity threats on four management sub-fields: strategic management; organisational theory; organisational behaviour, and human theory.

All 8 articles for the review on tourism and hospitality have been published in the last lustrum, from 2018 to 2023, highlighting the recency of the general topic and the timeliness of the review. Those results show some critical and worrisome data. Cybersecurity in tourism is much less developed than in management in general.

First, cybersecurity has not yet been recognised as a key issue in the ongoing discourse in tourism and hospitality. The lack of research on the topic could suggest barriers to its development. Problems in finding reliable data and being able to go deeper into the subject could be one of the main factors. In fact, both companies and individuals are reluctant to report such attacks in order to avoid visibility and losses in trust and brand reputation (Chen *et al.,* 2023).

Second, scientific leadership in terms of authors' productivity is quite dispersed. Thus, the ongoing discourse on cybersecurity in tourism and hospitality has not taken a very differentiated research direction as it remains anchored in the predominant keywords that are typical of very general cybersecurity issues (i.e. cyberattacks, cybercrimes, privacy, risk and data breach, and similar topics) with little or no depth by sub-sector, geographic area or type of tourism.

Third, thematic evolution has not yet been formed in tourism, which confirms that this topic in the tourism sector in still in its infancy this topic is in the tourism sector. Thematic evolution on cybersecurity in organisation, business, and management could provide some ideas regarding future research directions and applications in tourism and hospitality such as: artificial intelligence, blockchain, big data; cryptocurrencies; fraud phishing and social engineering related to data or human security, and user education applied to tourism. However, some authors emphasised that this problem is different between tourism and non-tourism companies; therefore, research could focus on other directions. Thus, like in other sectors with digital supply chains, cyber-supply chain risk management could convert into a critical discipline combining expertise from cybersecurity, supply chain management, and enterprise risk management in order to avoid breaches in operations (Boyson *et al.,* 2022).

Finally, human factors are a critical issue that do not appear in this systematic review analysis. Tourism industries are human capital intensive, so human failures can be an open door to malicious attacks. Generating a cyber security culture and capability is necessary to prevent breaches and theft of personal data of both employees and customers. In addition, education regarding the secure use of shared communication infrastructures for both customers and employees should reduce cybercrime problems.

In addition, although small businesses are more vulnerable to cyberattacks, no company is free from this type of delinquency. Especially in tourism industries, management teams are focused on their core business with little awareness of cybersecurity threats. Therefore, they do not expend money on cybersecurity protection because their technical knowledge in low (Boto-Garcia, 2023). Nevertheless, cybercrime is a killer for small companies when it happens (Incibe, 2023). Thus, investments in both tangible assets and human resources are needed to survive cyberattacks.

Another relevant issue in management is cybersecurity risk factor disclosure. As mentioned before, companies are reluctant to disclose cyberattacks. A company is more attractive for investment and reliability when it does not disclose problems regarding cybersecurity (Frank *et al*., 2023). The influence of disclosures, number of disclosures before and after the cyberattack, severity of the cyberattack, impacts on the company's attractiveness and reputation, and technical and operational measures are just some of the possible lines of inquiry that can be shared with management theory (Chen *et al*., 2022; Frank *et al*., 2023).

Innovation in companies can also be compromised when the dangers of security breaches are known. This knowledge may prevent risk-taking and innovation-oriented behaviour (Fusi *et al*., 2023). Tourism is recognised as an industry where a high degree of technological innovation coexists with traditional operational activities. But, as mentioned above, the management team usually has little knowledge of cybersecurity, which could precisely be a driving factor for innovation. The relationship between cybersecurity and innovativeness in tourism also should be studied as a strategic management approach.

This work has important implications for research, theory and practice, as it lays the groundwork to begin research on the topic from different theoretical and practical perspectives and approaches.

Thus, this study has emphasized several gaps and next steps for cybersecurity in tourism. They provide an opportunity to continue building research on this relevant topic for tourism.

Finally, this research is not without limitations. The most important is the small number of papers analyzed in the cybersecurity tourism sector. Although the reason is that more papers have not been published. This is an important limitation and, therefore, another bibliometric analysis should be conducted in the future, when the research on the topic has increased.

Funding details: This work was supported by the: Spanish Ministry of Universities, Recovery, Transformation and Resilience Plan, and the Autonomous University of Madrid under Grant CA2/RSUE/2021-00659; Chinese Ministry of Science and Technology and the University of Science and Technology of China, Hefei City, P.R.China under Grant DL2023200001L.

Disclosure statement: The authors report there are no competing interests to declare.

Data availability statement: Data used in this work are accessible from the Scopus database.

5. REFERENCES

ARIA, M. and CUCCURULLO, C. (2017): «Bibliometrix: An r-tool for comprehensive science mapping analysis », *Journal of Informetrics*, vol. 11 (4), pp. 959-975, https://doi.org/10.1016/j.joi.2017.08.007

BILEFSKY, D. (2017): «Hackers use new tactic at Austrian hotel: locking the doors», *The New York Times*, available at: www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html?_r=0 (accessed 31October 2023).

BORNMANN, L., MUTZ, R., NEUHAUS, C. and DANIEL, H. (2008): «Citation counts for research evaluation: standards of good practice for analyzing bibliometric data and presenting and interpreting results», *Ethics in Science and Environmental Politics*, vol. 8, pp. 93-102.

BOTO-GARCÍA, D. (2023): «Hospitality workers' awareness and training about the risks of online crime and the occurrence of cyberattacks», *Journal of Hospitality and Tourism Management*, vol. 55, pp. 240-247.

BOYSON, S., CORSI, T.M., and PARASKEVAS, J.P. (2022): «Defending digital supply chains: Evidence from a decade-long research program», *Technovation,* vol.118, p.102380.

BUTLER, J. (2016): «Not just heads in beds-cybersecurity for hotel owners», *Hospitality Net*, available at: www.hospitalitynet.org/opinion/4073687.html (accessed 31 October 2023):

CHEN, H. S. and FISCUS, J. (2018): «The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry», *Journal of Hospitality and Tourism Technology*, vol. 9 (2), pp. 223-234.

CHEN, J., HENRY, E. and JIANG, X. (2023): «Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach», *Journal of Business Ethics*, vol. 187 (1), pp.199-224.

DELGADO LÓPEZ-CÓZAR, E., ROBINSON-GARCÍA, N. and TORRES-SALINAS, D. (2014): «The Google scholar experiment: how to index false papers and manipulate bibliometric indicators», *Journal of the Association for Information Science and Technology*, vol. 65, pp. 446-454.

DENYER, D. and TRANFIELD, D. (2009): «Producing a systematic review», in D. A. Buchanan, A. Bryman (Eds.), *The SAGE handbook of organizational research methods*, pp. 671–689.

FRANCESCHINI, S., FARIA, L.G.D. and JUROWETZKI, R. (2016): «Unveiling scientific communities about sustainability and innovation. A bibliometric journey around sustainable terms», *Journal of Cleaner Production*, vol. 127, pp. 72-83.

FRANK, M.L., GRENIER, J.H., PYZOHA, J.S. and ZIELINSKI, N.B. (2023): «Implications of enhanced cybersecurity risk management reporting and independent assurance», *Current Issues in Auditing*, vol. 17 (1), pp. 11-18.

FUSI, F., JUNG, H. and WELCH, E. (2023): «Technological vulnerability and knowledge of cyber-incidents: Threats to innovativeness in local governments?», *Public Management Review*, p. 1-27. https://doi.org/10.1080/14719037.2023.2250362

GIGLIO, C., CORVELLO, V., CONIGLIO, I.M., KRAUS, S. and GAST, J. (2023a): «Cooperation between large companies and start-ups: An overview of the current state of research», *European Managment Journal*. https://doi.org/10.1016/j.emj.2023.08.002

GIGLIO, C., VOCATURO, G.S. and PALMIERI, R. (2023b): «A scientometric study of LCA-based industrialization and commercialization of geosynthetics in infrastructures», *Applied Sciences*, vol. 13 (4), p. 2328. https://doi.org/10.3390/app13042328

GIUSTINI, D. and KAMEL BOULOS, M.N. (2013): «Google Scholar is not enough to be used alone for systematic reviews», *Online Journal of Public Health Informatics*, vol. 5 (2), p. 214.

GWEBU, K., and BARROWS, C. W. (2020): «Data breaches in hospitality: is the industry different?», *Journal of Hospitality and Tourism Technology*, vol. 11 (3), pp. 511-527.

INCIBE (2023): Instituto Nacional de Ciberseguridad. Sala de Prensa. https://www.incibe.es. Revised on 30 October, 2023.

KOUSHA, K. and THELWALL, M. (2007): «Sources of Google Scholar citations outside the science citation index: a comparison between four science disciplines», *Scientometrics*, vol. 74 (2), pp. 273-294.

KRAUS, S., BREIER, M., LIM, W.M. *et al*. (2022): «Literature reviews as independent studies: guidelines for academic practice», *Review Managing Science*, vol. 16, pp. 2.577-2.595.

LASDA BERGMAN, E.M. (2012): «Finding citations to social work literature: the relative benefits of using web of science, Scopus, or Google scholar», *The Journal of Academic Librarianship*, vol. 38 (6), pp. 370-379.

LASO, P.M., SALMON, L., BOZHILOVA, M., IVANOV, I., STOIANOV, N., VELEV, G., CLARAMUNT., C. and YANAKIEV, Y. (2022): «ISOLA: An innovative approach to cyber threat detection in cruise shipping», in *Developments and Advances in Defense and Security: Proceedings of MICRADS 2021*. Singapore, Springer, pp. 71-81.

LOHRKE, F.T. and FROWNFELTER-LOHRKE, C. (2023): «Cybersecurity research from a management perspective: A systematic literature review and future research agenda», *Journal of General Management*, p. 03063070231200512. https://doi.org/10.1177/03063070231200512

MOHER, D., LIBERATI, A., TETZLA, J. and ALTMAN, D.G. (2009): «Preferred reporting items for systematic reviews and meta-analyses: The prisma statement», *Annals of Internal Medicine*, vol. 151, pp. 264-269, https://doi.org/10.7326/0003-4819-151-4-200908180-00135

PAGE, M. J., MCKENZIE, J. E., BOSSUYT, P. M., BOUTRON, I., HOFFMANN, T.C., MULROW, C. D., SHAMSEER, L., TETZLA, J. M., AKL, E. A., BRENNAN, S. E.,

CHOU, R., GLANVILLE, J., GRIMSHAW, J. M., HRÓBJARTSSON, A., LALU, M. M., LI, T., LODER, E. W., MAYO-WILSON, E., MCDONALD, S., … MOHER, D. (2021): «The prisma 2020 statement: An updated guideline for reporting systematic reviews», *BMJ*, vol. 372 (71), https://doi.org/10.1136/bmj.n71

PARASKEVAS, A. (2022): «Cybersecurity in travel and tourism: A risk-based approach», in *Handbook of e-Tourism*. Cham, Springer International Publishing, pp. 1.605-1.628.

PARSONS, F.J., PANTRIDGE, M.J. and FLAHERTY, G.T. (2021): «Cybersecurity risks and recommendations for international travellers», *Journal of Travel Medicine*, vol. 28 (8), pp. 1-4.

PITTAWAY, L., ROBERTSON, M., MUNIR, K., DENYER, D. and NEELY, A. (2004): «Networking and innovation: A systematic review of the evidence», *International Journal of Management Reviews*, vol. 5-6 (3-4), pp.137-168.

ROY, G.D. (2022): «Digital privacy concerns in India for medical tourism», *Journal of Public Affairs,* vol. 22, p. e2762.

SAHU, A.K. and GUTUB, A. (2022): «Improving grayscale steganography to protect personal information disclosure within hotel services», *Multimedia Tools and Applications*, vol. 81 (21), pp. 30.663-30.683.

SCHIEDERIG, T., TIETZE, F. and HERSTATT, C. (2012): «Green innovation in technology and innovation management: an exploratory literature review», *RandD Management*, vol. 42, pp. 180-192.

SECURITY (2023): «Travel and tourism sector ranked third in cyberattack incidents», *Security,* July 25th, 2024, available at https://www.securitymagazine.com/articles/99675-travel-and-tourism-sector-ranked-third-in-cyberattack-incidents [last accessed March 26th, 2024].

SIGALA, M. (2018): «New technologies in tourism: From multi-disciplinary to antidisciplinary advances and trajectories», *Tourism Management Perspectives*, vol. 25, pp. 151-155.

ZAHOOR, N., AL-TABBAA, O., KHAN, Z. and WOOD, G. (2020): «Collaboration and internationalization of SMEs: Insights and recommendations from a systematic review», *International Journal of Management Reviews*, vol. 22, pp. 427-456. https://doi.org/10.1111/ijmr.12238