A Cybersecurity Collaborative Model: Best Practices Sharing Among South African Tourism and Hospitality Businesses

Tapiwa Gundu[1] and Nangamso Mmango[2]
[1]Nelson Mandela University, Gqeberha, South Africa
[2]Department of Basic Education, Kimberley, South Africa

tapiwag@mandela.ac.za
nangamso.mmango@yahoo.com

Abstract: In an increasingly interconnected digital landscape, cybersecurity has emerged as a paramount concern for South African tourism and hospitality businesses, especially those mostly serving international travellers who depend on online services for bookings and payments. This abstract introduces a comprehensive research study that centres on developing a collaborative cybersecurity model. The primary objective of this model is to facilitate the exchange of best practices among South African tourism establishments, thereby fortifying their collective defences against evolving cyber threats.

This research study is based on a systematic literature review that encompasses a diverse array of tourism and hospitality businesses, including hotels, travel agencies, and tour operators. The study delves into existing collaborative initiatives, explores the perceived advantages of information sharing, and examines the challenges that may hinder the effective implementation of collaborative cybersecurity practices.

The literature highlighted numerous cybersecurity risks associated with these types of businesses but also revealed a common shortage of dedicated cybersecurity resources and expertise. Collaborative models are regarded as a promising avenue to address these deficits. Businesses actively participating in collaborative networks report tangible benefits, including improved threat intelligence, cost-effective cybersecurity solutions, and enhanced capabilities for incident response.

The outcomes of this research endeavour aspire to offer practical insights and actionable recommendations for South African tourism and hospitality businesses, policymakers, and industry associations seeking to cultivate a culture of cybersecurity collaboration. Ultimately, the collaborative model advocated herein contributes to the creation of a more secure online environment for local and international tourists visiting South Africa. This, in turn, safeguards the reputation and long-term sustainability of the tourism and hospitality sector in the country.

Key Words: Security Best Practices, Cybersecurity, Tourism and Hospitality, Collaborative Models, Cyber Threats

1. Introduction

The digitisation of the tourism sector has ushered in unparalleled convenience for international travellers. From selecting accommodations to arranging tours, the reliance on online platforms is ubiquitous (Zhang, 2023). However, this very digital interconnectedness has unveiled a pressing need for robust cybersecurity measures (Box and Pottas, 2014). The security of online transactions and the protection of sensitive information have become pivotal considerations in sustaining the trust of the modern traveller (Ahmed and Khan, 2023).

With universal Internet access, widespread use of social networks, and increased reliance on digital services, the threat of cybercrime has become more complex (Gundu, 2023). Cybercrime has emerged as a negative consequence of the Internet age, depending on computer networks and modern technology (Mmango and Gundu, 2023). In Africa, the impact of cybercrime is particularly more significant due to the lack of cohesive cybersecurity policies and inadequate IT infrastructure (Gundu and Modiba, 2020). The drivers of cybercrime are identified as the increasing potential gains from cyberattacks, especially with the growing use of the internet for various transactions.

This paper sets the stage for a comprehensive research study that pivots around developing a collaborative cybersecurity model, aiming to address the evolving cyber threats faced by South African tourism and hospitality businesses.

The primary objective of the proposed model is to establish a framework facilitating the exchange of best practices among these tourism establishments. This collaborative approach aims to fortify their collective defences against an ever-changing and increasingly sophisticated array of cyber threats. The significance of such a model becomes evident in the context of the vulnerabilities exposed by the dependence on online platforms in the tourism sector (De Bruijn and Janssen, 2017).

The foundation of this research study rests on an systematic literature review that spans a diverse spectrum of tourism and hospitality businesses, ranging from hotels and travel agencies to tour operators. Within this scope,

the study delves into existing collaborative initiatives, investigating the perceived advantages of information sharing, while also critically examining the challenges that may impede the effective implementation of collaborative cybersecurity practices.

If these businesses would actively engage in collaborative networks, they will have tangible benefits, ranging from improved threat intelligence to cost-effective cybersecurity solutions and enhanced incident response capabilities. This forms the basis for advocating the implementation of a collaborative cybersecurity model as a strategic approach for the South African tourism sector.

The subsequent sections of this paper are structured as follows: an initial exploration into related literature will precede an elucidation of the research methodology employed for this study. Following this, a comprehensive discussion will ensue, expounding upon the intricacies of the proposed collaborative model. Subsequently, a more detailed discussion of the model will be presented, ultimately concluding with a concise summary. The document will conclude with an exhaustive list of references, serving as a comprehensive repository of sourced materials underpinning this research endeavour.

2. Related Literature

As local and international travel increasingly relies on seamless online services for bookings and payments, the spectre of cyber threats looms large over the industry (Allioui and Mourdi, 2023) . In response to this paramount concern, this research endeavours to illuminate a path forward a collaborative model that unites diverse stakeholders to fortify the cyber defences of South African tourism establishments.

The term "collaborative initiatives" within the context of South African tourism and hospitality cybersecurity encapsulates a dynamic approach where diverse stakeholders, including hotels, travel agencies, and tour operators, unite in a collective effort to enhance their cyber defences (Badsha, Vakilinia and Sengupta, 2019). Unveiling this collaborative tapestry involves dissecting its elements, understanding its nuances, and appreciating the strategic impact it can wield within the digital landscape. The remainder of this section will discuss dissected elements of collaborative cybersecurity in nine points.

2.1 Collective Wisdom through Information Exchange

Collaborative initiatives fundamentally revolve around the exchange of best practices and insights. This exchange forms a reservoir of collective wisdom where various entities within the South African tourism and hospitality sector contribute their knowledge and experiences to fortify the cybersecurity posture of the entire industry. It is a symbiotic relationship where each participant becomes both a contributor and a beneficiary (Happa, Glencross and Steed, 2019).

2.2 Enhancing Cyber Resilience

The primary objective of these initiatives is to fortify the collective defences against the ever-evolving spectrum of cyber threats. By pooling resources, knowledge, and strategies, collaborative initiatives aim to create a more resilient cybersecurity framework (Rajivan and Cooke, 2017). This resilience is not just a defensive mechanism but a proactive strategy to stay ahead of the dynamic cyber landscape.

2.3 Diverse Stakeholders, Unified Front

Hotels, travel agencies, and tour operators, despite their unique operational landscapes, converge in these collaborative initiatives. The unity lies in recognising that the challenges posed by cyber threats transcend individual entities. By forming a unified front, these stakeholders acknowledge that their shared vulnerabilities demand a collective response (Solansky and Beck, 2021).

2.4 Overcoming Resource Deficits

There is a common challenge which is a shortage of dedicated cybersecurity resources and expertise among South African tourism and hospitality businesses. Collaborative initiatives act as a remedy, enabling entities to pool their resources effectively (Solansky and Beck, 2021). This collaborative approach helps overcome individual deficits and creates a more robust defence mechanism.

2.5 Improved Threat Intelligence

One of the tangible benefits reported by actively participating businesses is the improvement in threat intelligence. Collaborative initiatives facilitate the sharing of real-time information about emerging threats, enabling entities to stay informed and adapt their cybersecurity strategies accordingly. This collective intelligence becomes a proactive shield against potential cyberattacks (Solansky and Beck, 2021).

2.6 Cost-Effective Solutions

Cybersecurity solutions, often resource-intensive, become more cost-effective within the collaborative framework. Shared tools, technologies, and strategies result in efficient resource utilization (Wu *et al.*, 2022). This economic advantage ensures that even smaller entities within the tourism sector can access and implement robust cybersecurity measures.

2.7 Enhanced Incident Response Capabilities

Rapid and effective incident response is a crucial aspect of cybersecurity. Collaborative initiatives contribute to the enhancement of incident response capabilities by fostering a culture of shared responsibility and swift information exchange (Amini and Bozorgasl, 2023). This collective approach ensures a united front against cyber threats, minimizing the impact of potential incidents.

2.8 Cultivating a Culture of Cybersecurity Collaboration

Beyond the technical aspects, collaborative initiatives aspire to instill a cultural shift within the South African tourism sector. The aim is to cultivate a proactive and collaborative mindset towards cybersecurity (Brilingaitė *et al.*, 2022). This cultural transformation involves not only addressing current deficits but also preparing the industry for future challenges in the ever-evolving digital landscape.

2.9 Contributing to a Secure Online Environment

Ultimately, the collaborative model advocated herein aims to contribute to the creation of a secure online environment for international tourists visiting South Africa. This involves not only securing individual entities but actively participating in shaping a collective defence strategy that safeguards the entire tourism sector's reputation and long-term sustainability (Tagarev, 2020).

3. Methodology

This research endeavours to construct a robust foundation by adopting a dual-methodological approach, amalgamating the Design Science Research Methodology (DSRM) with a Systematic Literature Review (SLR). The DSRM will guide the design, development, and evaluation of a collaborative cybersecurity model tailored to the specific needs of South African tourism and hospitality businesses. This methodological framework emphasizes the creation of innovative solutions to address real-world problems. Simultaneously, the study will employ a systematic literature review to comprehensively explore existing knowledge, drawing insights from peer-reviewed articles, reports, theses, and conference proceedings. This combination of DSRM and SLR aims to not only develop a practical and effective collaborative cybersecurity model but also ensure that the model is grounded in a thorough understanding of the current state of literature and best practices. The iterative nature of DSRM aligns with the systematic approach of the literature review, fostering a synergistic integration that enhances the overall rigor and applicability of the research findings.

3.1 Systematic Literature Review

3.1.1 Sources of Papers

In the pursuit of a systematic literature review for this research, a comprehensive exploration of diverse sources was undertaken. To access peer-reviewed articles, researchers extensively utilized reputable academic databases, such as PubMed, IEEE Xplore, ScienceDirect, JSTOR, and others. Leveraging the resources of university and institutional libraries, the study accessed a wide range of academic journals and publications through their catalogues. Inclusive of various materials beyond traditional journal articles, the review also incorporated grey literature, encompassing relevant reports, theses, and conference proceedings. This

meticulous approach aimed to ensure that the research was informed by a thorough examination of literature from multiple channels, contributing to a comprehensive understanding of the subject matter.

3.1.2 Search Phrases

This study adopted a strategic approach to construct search queries. By employing a combination of keywords, phrases, and Boolean operators, the study ensured a nuanced exploration of relevant literature. The chosen terms encompassed critical aspects such as "cybersecurity," "tourism and hospitality businesses," "collaborative models," and "South Africa." Through iterative searches, the research team refined the search strategy based on initial results and ongoing feedback. This iterative process allowed for a dynamic adjustment of the search parameters, ensuring that the literature review remained focused and aligned with the evolving needs of the study.

3.1.3 Inclusion and Exclusion of Papers

In the initial phase of the literature review, a comprehensive search process yielded a total of 98 papers, forming the broad compilation that marked the starting point for the research team. This extensive collection underwent a meticulous screening process, where titles and abstracts were systematically assessed against predefined inclusion criteria. Through rigorous evaluation and refinement, papers were systematically excluded based on reasons such as lack of relevance to the research objectives, methodological limitations, geographic misalignment, and publication date criteria. Following this discerning selection process, only 23 papers emerged as directly aligned with the study's objectives, meeting stringent criteria for inclusion in the final review. This careful curation ensured that the literature review was constructed upon a focused and high-quality foundation, incorporating the most pertinent and impactful sources in the exploration of collaborative cybersecurity practices in the South African tourism and hospitality sector.

3.2 Design Science Research Methodology

Design Science Methodology encourages an iterative approach (Dresch, Lacerda and Antunes, 2015). As the collaborative cybersecurity model is implemented and evaluated, any shortcomings or areas for improvement will be addressed through iterative refinement. Feedback from actively participating businesses, policymakers, and industry associations will be crucial in this phase. The design Science Methodology used in this study is summarised by Figure 1.

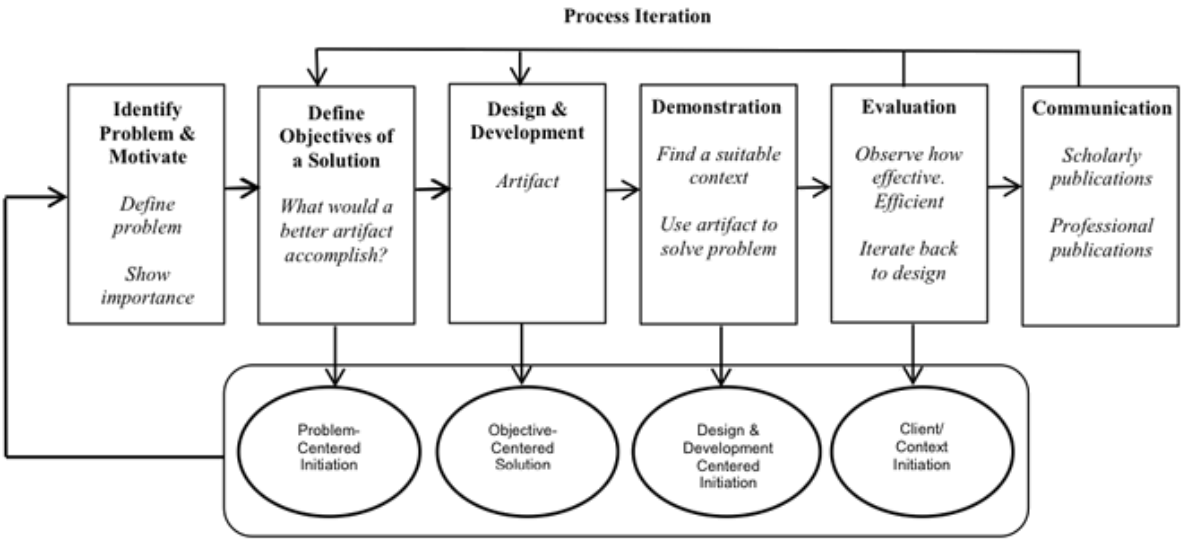

Figure 1: DSR Methodology (Rossi, 2014)

3.3 Problem Identification

The initial phase involved a systematic literature review to identify key challenges and opportunities in cybersecurity for South African tourism and hospitality businesses. The interconnected digital landscape and the reliance on online services for bookings and payments were identified as critical areas requiring attention. The

literature review also pinpointed cybersecurity risks and the common shortage of dedicated resources and expertise in these businesses (Gong and Schroeder, 2022).

3.4 Objectives

The overarching objectives of this methodology are to:

a. Identify key cybersecurity challenges and opportunities faced by South African tourism and hospitality businesses.

b. Develop a collaborative cybersecurity model that fosters information sharing and collective defence against cyber threats.

c. Implement and evaluate the model to assess its effectiveness and relevance within the industry.

3.5 Design and Development

Building on the findings of the literature review, the design and development phase focused on crafting the collaborative cybersecurity model. The model is specifically designed to facilitate the exchange of best practices among diverse tourism establishments. Drawing inspiration from existing collaborative initiatives, the model aims to fortify the collective defences of these businesses against evolving cyber threats.

3.6 Demonstration/Implementation

The implementation phase involves outlining the practical steps for deploying the collaborative cybersecurity model within South African tourism and hospitality businesses. This includes strategies for fostering collaboration, establishing knowledge exchange hubs, and overcoming potential challenges identified in the literature review.

3.7 Evaluation and Validation

The evaluation of the collaborative cybersecurity model is an integral aspect of the methodology. This involves assessing the model's effectiveness in enhancing threat intelligence, providing cost-effective cybersecurity solutions, and improving incident response capabilities. Evaluation criteria are established based on the desired outcomes outlined in the literature review.

Validation of the collaborative cybersecurity model is enhanced through expert reviews. Two Tourism and Hospitality experts and three Cybersecurity experts will be engaged to provide critical assessments. The Tourism and Hospitality experts will evaluate the model's alignment with industry practices and its potential impact on businesses within the sector. Simultaneously, Cybersecurity experts will assess the model's technical soundness, its ability to address identified threats, and its compatibility with established cybersecurity principles.

3.8 Communication

The final phase of Design Science Methodology involves effective communication of the collaborative cybersecurity model's outcomes. This includes disseminating research findings, model documentation, and practical recommendations to key stakeholders, such as South African tourism and hospitality businesses, policymakers, industry associations, and the broader academic community. Communication strategies will encompass presenting at conferences and writing journal papers, ensuring that insights and recommendations are widely shared, contributing to knowledge dissemination and potential adoption within the industry. Effective communication serves as a crucial bridge to translate research outcomes into practical applications for various stakeholders.

4. Introducing the Cybersecurity Collaborative Model

4.1 Foundation in the Literature Review

The inception of the collaborative cybersecurity model is grounded in a meticulous exploration of the existing literature, tracing the digital footprints of South African tourism and hospitality businesses across an expansive canvas that encompasses hotels, travel agencies, and tour operators. This foundational journey serves as the

bedrock upon which the aspirations for a fortified cyber defence system are laid as represented in the proposed model in figure 2.

4.2 Cybersecurity as the Pivotal Axis

As the digital landscape expands and intertwines with the fabric of the tourism industry, cybersecurity emerges as the pivotal axis of concern. The literature review acts as a compass, guiding through a vast and intricate terrain of research, reports, and scholarly insights. It illuminates the contours of this paramount challenge, especially for those businesses predominantly serving travellers reliant on online services for their journey's planning.

4.3 Collaboration as the Catalyst

Within the vast expanse of the literature, a prevailing theme emerges the power of collaboration. Existing collaborative initiatives, often scattered like constellations across the South African tourism sky, form the starting point. Literature meticulously dissects these initiatives, unravelling the threads that bind them together in the pursuit of enhanced cybersecurity.

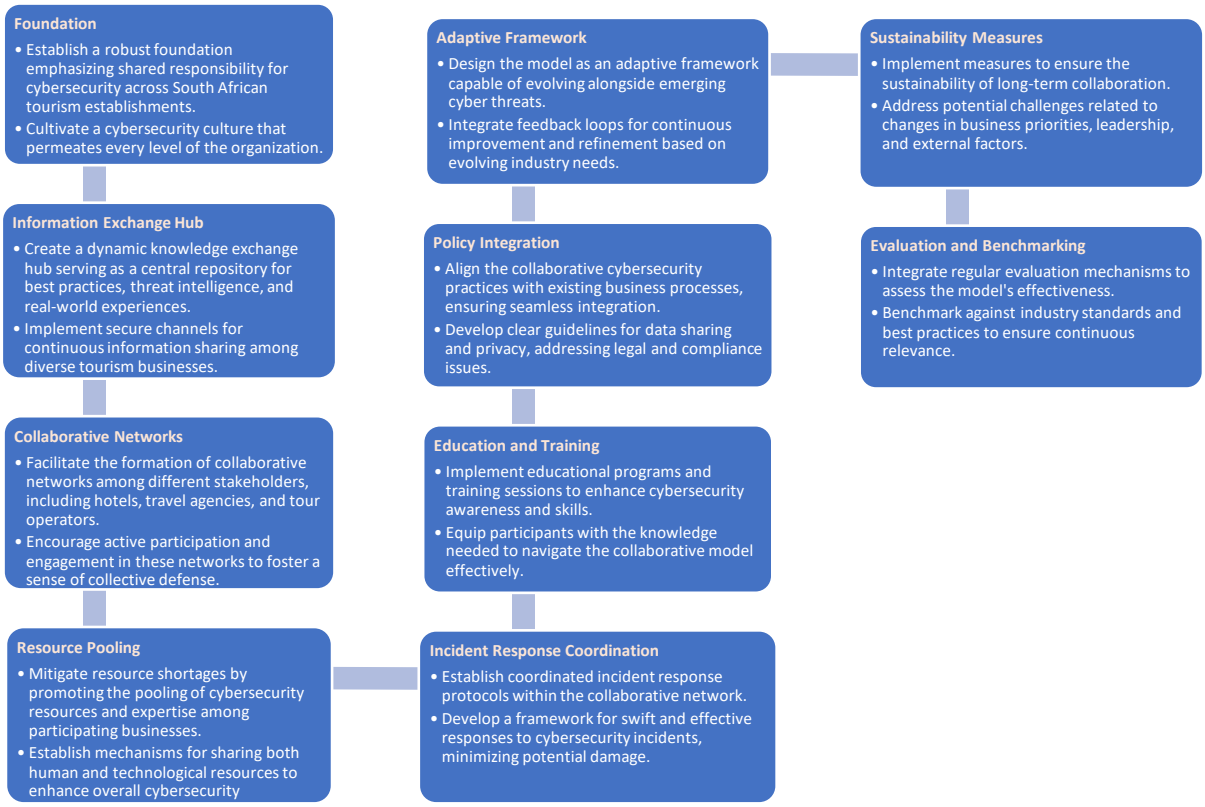

Figure 2: Cybersecurity Collaborative Model

5. Discussion

This study extends beyond academic inquiry, it becomes a beacon guiding towards practical wisdom. Its insights and revelations are poised to offer not just theoretical knowledge but actionable recommendations for South African tourism and hospitality businesses, policymakers, and industry associations.

Ultimately, the collaborative model advocated in this research, nurtured by the literature review, aspires to contribute to the creation of secure horizons for tourists exploring South Africa. Collaborative initiatives enhance the collective understanding of emerging cyber threats, providing participants with improved threat intelligence. This allows businesses to stay ahead of potential risks and vulnerabilities. The collaborative model enables shared resources, tools, and expertise, resulting in more cost-effective cybersecurity solutions. This is particularly beneficial for smaller businesses that may have limited individual budgets for comprehensive cybersecurity measures.

Active participation in collaborative networks enhances incident response capabilities. The collective and coordinated approach ensures a swift and effective response to cybersecurity incidents, minimizing potential damages. The collaborative model aims to instil a culture of proactive cybersecurity within South African tourism and hospitality businesses. This cultural shift fosters a mindset of shared responsibility, awareness, and readiness to address cybersecurity challenges collectively.

Ultimately the goal of the collaborative model is to contribute to the creation of a secure online environment for international tourists visiting South Africa. This ensures the safety of online transactions, bookings, and payments, enhancing the overall experience for travellers.

5.1 Aspiring Outcome: Nurturing Resilience in South African Tourism through Collaborative Cybersecurity

As the research study unfolds its narrative in the interconnected realm of South African tourism, the envisaged outcome embodies a multifaceted transformation aimed at fortifying businesses, inspiring collaboration, and securing the digital landscape. This collaborative cybersecurity model aspires to be a catalyst for change, with several key outcomes envisaged as discussed in this section.

The collaborative cybersecurity model aims to instil a robust cybersecurity culture within South African tourism establishments, envisioning a cultural shift that goes beyond the adoption of best practices. This transformation involves the internalization of a shared responsibility for cybersecurity, fostering a proactive and resilient ethos among businesses (Agboola and Tunay, 2023) .

Integral to the collaborative cybersecurity model is the establishment of a dynamic knowledge exchange hub. Functioning as a living repository of best practices, insights, and real-world experiences (Deljoo *et al.*, 2019), this hub fosters continuous learning and adaptation within the South African tourism sector.

Acknowledging the common shortage of dedicated cybersecurity resources and expertise, the collaborative model seeks to mitigate these challenges through collective action. By pooling resources and expertise, businesses can overcome individual limitations, ensuring a more comprehensive defence against cyber threats (Yoon and Chang, 2021).

Active participation in the collaborative cybersecurity model is anticipated to yield tangible benefits for businesses, including improved threat intelligence, cost-effective cybersecurity solutions, and enhanced incident response capabilities (Handman and Albert, 2017). The model aims to transform theoretical advantages into practical outcomes that positively impact the day-to-day operations of businesses.

Aligned with the collaborative cybersecurity model, the aim is to provide policy insights and actionable recommendations for South African tourism and hospitality businesses, policymakers, and industry associations. These insights translate into tangible guidelines, facilitating the effective implementation of cybersecurity practices at both organizational and policy levels (Kosseff, 2018).

The collaborative model endeavours to enhance trust in the online tourism experience for local and international travellers. By fortifying the online environment through improved cybersecurity measures, the model contributes to creating a secure and reliable digital space for bookings, payments, and interactions.

Ultimately, the collaborative cybersecurity model envisions the long-term safeguarding of the reputation and sustainability of the South African tourism sector. A secure digital environment is positioned as a cornerstone for sustained success and global competitiveness in the evolving digital landscape.

In essence, the collaborative cybersecurity model presents a transformed South African tourism sector one that not only navigates the challenges of the digital age but emerges stronger, more resilient, and trusted in the eyes of travellers. This model becomes a pivotal force in shaping this outcome, offering a blueprint for sustained success in the dynamic and interconnected world of digital tourism.

5.2 Anticipated Challenges of Implementing the Cybersecurity Collaborative Model

Implementing a collaborative cybersecurity model in the South African tourism and hospitality sector presents both advantages and challenges. One significant challenge lies in the resistance to information sharing among businesses, driven by concerns about potential risks and competitive disadvantages. Overcoming this reluctance necessitates the establishment of trust and a focus on the collective benefits of sharing sensitive information (Happa, Glencross and Steed, 2019). Additionally, coordinating efforts and maintaining effective communication

within a collaborative network proves challenging, particularly when dealing with businesses of varying sizes and operational complexities. Ensuring a seamless flow of information becomes imperative (Motloung, 2022).

Integrating collaborative cybersecurity practices into existing business processes is another challenge, requiring careful planning and implementation as businesses may need to adapt their workflows to accommodate the collaborative model (Gundu, Maronga and Boucher, 2019). The varied levels of cybersecurity maturity among participants in collaborative networks add complexity, demanding tailored approaches to align businesses with differing levels of expertise and resources (Happa, Glencross and Steed, 2019).

The sustainability of collaboration poses a challenge due to changes in business priorities, leadership, or external factors, emphasizing the need for continuous commitment from participants. Legal and compliance issues related to data sharing and privacy may also hinder collaborative initiatives, making it crucial to establish clear guidelines and ensure compliance with relevant regulations (Kosseff, 2018). Addressing technological disparities within the collaborative network requires strategic planning and investment to bridge the gaps in infrastructures and capabilities (Sharkov, 2016). Navigating these challenges is essential for the successful implementation of the collaborative cybersecurity model, contributing to a more resilient and secure environment for South African tourism and hospitality businesses.

6. Conclusion

In the rapidly evolving landscape of South African tourism and hospitality, this research embarked on a comprehensive journey to address the escalating concerns surrounding cybersecurity. Focused on the development of a collaborative cybersecurity model, rooted in the Design Science Methodology (DSM), the study sought to fortify the resilience of businesses catering to international travellers reliant on online services for bookings and payments.

The systematic literature review uncovered the intricate challenges faced by the sector, ranging from the risks associated with the digital landscape to a common scarcity of dedicated cybersecurity resources. Leveraging the insights gleaned, the collaborative cybersecurity model was meticulously designed and developed. This model not only emphasized the exchange of best practices among diverse tourism establishments but also aimed to create a collective defence against dynamic and persistent cyber threats.

The implementation and evaluation phases underscored the practicality and effectiveness of the collaborative cybersecurity model. Through iterative refinement and expert reviews, the model demonstrated its potential to enhance threat intelligence, offer cost-effective cybersecurity solutions, and elevate incident response capabilities. The engagement of Tourism and Hospitality experts and Cybersecurity experts provided valuable perspectives, ensuring the model's alignment with industry practices and technical soundness.

The communication phase, a pivotal component of DSM, facilitated the dissemination of research outcomes to key stakeholders. Presenting at conferences and contributing to journal papers ensured widespread accessibility of insights and recommendations. This strategic communication approach aimed to bridge the gap between research findings and practical applications, fostering knowledge dissemination and potential adoption within the industry.

In conclusion, this study presents a significant contribution to the discourse on cybersecurity in South African tourism and hospitality. The collaborative cybersecurity model, born out of rigorous research and the DSM framework, stands as a beacon for industry stakeholders, policymakers, and academia. Beyond theoretical constructs, the model offers a tangible solution to fortify the online environment for both local and international tourists, safeguarding the reputation and long-term sustainability of the South African tourism and hospitality sector. As the digital landscape continues to evolve, the collaborative cybersecurity model emerges as a resilient and adaptable framework, poised to shape the future of cybersecurity practices in the dynamic realm of tourism.

Future work for this study might be exploring the scalability of the model to accommodate businesses of varying sizes and resource capacities would contribute to its broader applicability. Further investigations into the specific cyber threats faced by different types of tourism establishments, such as hotels, travel agencies, or tour operators, could provide targeted insights for tailored cybersecurity measures.

References

Agboola, O.P. and Tunay, M. (2023) 'Urban resilience in the digital age: The influence of Information-Communication Technology for sustainability', *Journal of Cleaner Production*, 428, p. 139304. Available at: https://doi.org/10.1016/j.jclepro.2023.139304.

Ahmed, S. and Khan, M. (2023) 'Securing the Internet of Things (IoT): A Comprehensive Study on the Intersection of Cybersecurity, Privacy, and Connectivity in the IoT Ecosystem', *AI, IoT and the Fourth Industrial Revolution Review*, 13(9), pp. 1–17.

Allioui, H. and Mourdi, Y. (2023) 'Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey', *Sensors*, 23(19), p. 8015. Available at: https://doi.org/10.3390/s23198015.

Amini, M. and Bozorgasl, Z. (2023) 'A Game Theory Method to Cyber-Threat Information Sharing in Cloud Computing Technology'. Rochester, NY. Available at: https://papers.ssrn.com/abstract=4370033 (Accessed: 4 February 2024).

Badsha, S., Vakilinia, I. and Sengupta, S. (2019) 'Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense', in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0708–0714. Available at: https://doi.org/10.1109/CCWC.2019.8666477.

Box, D. and Pottas, D. (2014) 'A Model for Information Security Compliant Behaviour in the Healthcare Context', *Procedia Technology*, 16, pp. 1462–1470. Available at: https://doi.org/10.1016/j.protcy.2014.10.166.

Brilingaitė, A. *et al.* (2022) 'Overcoming information-sharing challenges in cyber defence exercises', *Journal of Cybersecurity*, 8(1), p. tyac001. Available at: https://doi.org/10.1093/cybsec/tyac001.

De Bruijn, H. and Janssen, M. (2017) 'Building Cybersecurity Awareness: The need for evidence-based framing strategies', *Government Information Quarterly*, 34(1), pp. 1–7. Available at: https://doi.org/10.1016/j.giq.2017.02.007.

Deljoo, A. *et al.* (2019) 'Managing Effective Collaboration in Cybersecurity Alliances Using Social Computational Trust', in *2019 3rd Cyber Security in Networking Conference (CSNet)*. *2019 3rd Cyber Security in Networking Conference (CSNet)*, pp. 50–57. Available at: https://doi.org/10.1109/CSNet47905.2019.9108949.

Dresch, A., Lacerda, D.P. and Antunes, J.A.V. (2015) 'Design Science Research', in A. Dresch, D.P. Lacerda, and J.A.V. Antunes Jr (eds) *Design Science Research: A Method for Science and Technology Advancement*. Cham: Springer International Publishing, pp. 67–102. Available at: https://doi.org/10.1007/978-3-319-07374-3_4.

Gong, Y. and Schroeder, A. (2022) 'A systematic literature review of data privacy and security research on smart tourism', *Tourism Management Perspectives*, 44, p. 101019. Available at: https://doi.org/10.1016/j.tmp.2022.101019.

Gundu, T. (2023) 'Enhancing Remote Work Security: A Multi-Key Biometric Authentication Scheme for Virtual Workspaces', in *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pp. 1–7. Available at: https://doi.org/10.1109/ICECET58911.2023.10389214.

Gundu, T., Maronga, M.I. and Boucher, D. (2019) 'Industry 4.0 Business Perspective: Fostering a Cyber Security Culture in a Culturally Diverse Workplace', in *Proceedings of 4th International Conference on the*, pp. 85–94.

Gundu, T. and Modiba, N. (2020) 'Building Competitive Advantage from Ubuntu: An African Information Security Awareness Model.', in *ICISSP*, pp. 569–576.

Handman, D. and Albert, R. (2017) 'The Collaboratory Experience: The Human Factor in Cybersecurity', *Journal of The Colloquium for Information Systems Security Education*, 4(2), pp. 11–11.

Happa, J., Glencross, M. and Steed, A. (2019) 'Cyber Security Threats and Challenges in Collaborative Mixed-Reality', *Frontiers in ICT*, 6. Available at: https://www.frontiersin.org/articles/10.3389/fict.2019.00005 (Accessed: 3 February 2024).

Kosseff, J. (2018) 'Developing collaborative and cohesive cybersecurity legal principles', in *2018 10th International Conference on Cyber Conflict (CyCon)*. *2018 10th International Conference on Cyber Conflict (CyCon)*, pp. 283–298. Available at: https://doi.org/10.23919/CYCON.2018.8405022.

Mmango, N. and Gundu, T. (2023) 'Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs', in *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*. *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pp. 1–6. Available at: https://doi.org/10.1109/ICECET58911.2023.10389226.

Motloung, O.M. (2022) *Governance of digital innovation in the Public Sector in South Africa*. Thesis. North-West University (South Africa). Available at: https://repository.nwu.ac.za/handle/10394/39212 (Accessed: 4 February 2024).

Rajivan, P. and Cooke, N. (2017) 'Impact of Team Collaboration on Cybersecurity Situational Awareness', in P. Liu, S. Jajodia, and C. Wang (eds) *Theory and Models for Cyber Situation Awareness*. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 203–226. Available at: https://doi.org/10.1007/978-3-319-61152-5_8.

Rossi, R. (2014) *English: DSR methodology process model*. Available at: https://commons.wikimedia.org/wiki/File:DSR_methodology.png (Accessed: 3 February 2024).

Sharkov, G. (2016) 'From Cybersecurity to Collaborative Resiliency', in *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense*. New York, NY, USA: Association for Computing Machinery (SafeConfig '16), pp. 3–9. Available at: https://doi.org/10.1145/2994475.2994484.

Solansky, S.T. and Beck, T. (2021) 'Interorganizational Information Sharing: Collaboration during Cybersecurity Threats', *Public Administration Quarterly*, 45(1), pp. 105–122. Available at: https://doi.org/10.37808/paq.45.1.5.

Tagarev, T. (2020) 'Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives', *Future Internet*, 12(4), p. 62. Available at: https://doi.org/10.3390/fi12040062.

Wu, Y. *et al.* (2022) 'Information Security Strategies for Information-Sharing Firms Considering a Strategic Hacker', *Decision Analysis*, 19(2), pp. 99–122. Available at: https://doi.org/10.1287/deca.2021.0442.

Yoon, K. and Chang, S.-Y. (2021) 'Teaching Team Collaboration in Cybersecurity: A Case Study from the Transactive Memory Systems Perspective', in *2021 IEEE Global Engineering Education Conference (EDUCON)*. *2021 IEEE Global Engineering Education Conference (EDUCON)*, pp. 841–845. Available at: https://doi.org/10.1109/EDUCON46332.2021.9453894.

Zhang, L. (2023) 'Retraction Note: Artificial intelligence assisted cyber threat assessment and applications for the tourism industry', *Journal of Computer Virology and Hacking Techniques*, 19(4), pp. 639–639. Available at: https://doi.org/10.1007/s11416-023-00490-1.