International Journal of Hospitality and Tourism Systems
Volume 18 Issue 4 2025
ISSN: 0974-6250 (Print)

https://doi.org/10.21863/ijhts/2025.18.4.003

Hospitality & Tourism Systems

Cyber Threats and Digital Security Challenges Facing SMEs in Cappadocia's Tourism Industry

Koray Çamlıca*, Eda Özgül Katlav**

Abstract *Purpose: To identify key factors influencing the implementation of cybersecurity practices in SMEs and assess the preparedness and obstacles these businesses encounter in adopting effective cybersecurity measures.*

Methodology/Design/Approach: A statistical analysis was conducted to evaluate the cybersecurity awareness among SME staff and to identify common barriers such as budget constraints, time limitations, and personnel shortages impacting cybersecurity initiatives.

Findings: The findings reveal that the majority of SME staff possess only limited awareness of cybersecurity implications, with a notable lack of high-level awareness. Additionally, budget constraints and time limitations were identified as significant barriers to adopting cybersecurity measures. The results underscore the necessity for recruitment and training initiatives to enhance cybersecurity awareness among staff.

Originality of the Research: This research contributes to the existing literature on cybersecurity by focusing specifically on small and medium-sized enterprises (SMEs) within the unique context of Cappadocia's tourism industry.

Keywords: *Cybersecurity, SMEs, Tourism Industry, Cappadocia, Awareness Levels, Implementation Challenge*

INTRODUCTION

One of the most historically significant and architecturally unique regions in Turkey is called Cappadocia located in the central part of the country (Günden & Günden, 2022). Cappadocia's rock-cut churches and fantastic structures called 'fairy chimneys' attract millions of tourists (De Pascale et al., 2023). It can be found top of the list of UNESCO World Heritage sites and is fundamentally involved in cultural and adventure tourism, which has built a sustainable economy having a focus on SMEs, like hotels, restaurants, shops for arts and crafts, tour operators, etc (Öztürk Büke, 2023). These SMEs are the main stakeholders in Cappadocia's tourism sector, as they offer value-added, culturally charged services in a competitive setting of large firms (Büyükkuru & Yılmaz, 2022).

As the world's popularity for tourism grows, Cappadocia's tourism industry has broadened its utilization of digital resources for business functioning, clients' communications, and marketing (Ardıç Yetiş et al., 2022). The advent of COVID-19 hastened this transition, improving SME visibility and transactions. Nevertheless, such a shift has made the businesses vulnerable to cyber risks; something that many SMEs find hard to deal with due to lack of capital (Yetiş et al.; Yigit Ozkan & Spruit, 2023). These and similar forms of digital risks such as phishing, and ransomware involve customer data and pose threats to financial stability, as well as, business reputation (Asgary et al., 2020; Kumar, et al. , 2025; Bouramdane, 2023). As the customer is the centerpiece of the businesses in the industry, small infringements could also result in great losses and this shows that the industry demands robust cybersecurity

* Faculty of Tourism, Nevsehir Haci Bektas Veli University, Turkey. Email: koraycamlica@nevsehir.edu.tr; https://orcid.org/0000-0003-0746-285X (Corresponding author)
** Faculty of Tourism, Nevsehir Haci Bektas Veli University, Turkey. Email: edaozgul@nevsehir.edu.tr; ORCiD: https://orcid.org/0000-0002-4168-909X

measures, and the organization must be ready and capable of responding to cyber incidents (Arroyabe et al., 2024; Özen, 2020).

However, even in this critical time, the majority of SMEs are still ignorant, inexperienced, and underfunded to support protective measures (Benz & Chatterjee, 2020; Yağcı et al., 2020). Research has indicated that the SMEs operating in the tourism sector are relatively ill-equipped when it comes to cybersecurity, they lack the resources to invest in sophisticated technical securities and their employees receive minimal training on how to handle cyber threats (Eldem, 2020). These vulnerabilities are only worsened by resource limitations; such that small businesses might forgo investing in more substantive security measures in favor of addressing present exigencies (Aydın & Akpınar, 2023). Nonetheless, since cyber threats can lead to severe economic consequences for the organizations in question, cybersecurity has to become a core component of digital agendas in these companies (Asgary & Ozdemir, 2020).

Noting these challenges, the present study seeks to identify the exact nature of cyber threats to Cappadocia's tourism SMEs and examine how these businesses can enhance their security against cyber threats (Tariq, 2024). Thus, the objective of this research is to analyze the frequency and consequences of cyber threats affecting operational continuity and to recommend specific preventive measures that apply to SMEs in the tourism sector. This line of research investigating cybersecurity in tourism, this research offers new findings and practical recommendations for protecting firms' digital resources, which are relevant to the sustainable development of Cappadocia's tourism industry.

LITERATURE REVIEW

Evaluating the current literature, the researchers of the current study have extracted the most relevant and updated scholarly work that gives further insights into the research topic and provides a clearer perspective on the existing research gaps.

Cybersecurity Perceptions and Preparedness in SMEs

A study by Wilson et al. (2022) aimed to study the state of SMEs' cybersecurity attitudes and determined that while the awareness of cyber threats does exist, there is a gap between the management's perception of such threats and the adoption of security measures. The survey of 206 UK-based SMEs showed that these companies understood some potential impacts of cyber attacks but underestimated the probability of the attack. Chidukwani et al. (2022) also found that SMEs in general invest in "Identify" and "Protect" controls while paying minimal attention to "Detect," "Respond," and "Recover" measures; hence, the need for more encompassing cybersecurity strategies.

Phishing and malware were also separately explored by Alkhalil et al. (2021) and Li and Liu (2021) and were revealed to be crucial to customer-oriented industries like tourism (Li & Liu, 2021). Similar to Alkhalil et al., who pointed out that SMEs are exposed to digital threats because they engage in numerous digital interactions, Florido-Benítez (2024) described data vulnerability in online travel agencies and hotels. These studies imply that although the threats involved in phishing risks are known, little has been done to investigate the effects of such threats in tourism SMEs dominated by the importance of data handling (Yigit Ozkan & Spruit, 2023).

Sector-Specific Vulnerabilities and the Role of Digital Readiness

The COVID-19 pandemic has exposed the weaknesses of SMEs in the tourism sector; However, the use of new technologies also brings new threats, as Florido-Benítez (2024) and Dayour et al. (2023) pointed out. Dayour et al. noted that in the Ghanaian tourism industry, ICT use enhances competitive advantage and cyber risks. For instance, Kraj et al. (2022) revealed that digital readiness was comparatively low among the Czech SMEs, and thus, the tourism SMEs are equally struggling to adopt the right mix of digital with cybersecurity solutions. This gap for Cappadocia's tourism SMEs implies the need for strategies that respond to sector-specific cybersecurity while promoting digital competitiveness.

Crisis Management and Cybersecurity in the Context of Tourism SMEs

Crisis management in tourism SMEs is a popular subject; Kukanja et al. (2020) and Gregurec et al. (2021) focus on how these businesses faced the COVID-19 crisis. The research by Kukanja on Slovenian tourism SMEs reveals that businesses have focused on people and costs and have not paid attention to cyber risk management even though they have relied on digital solutions during the pandemic (Kukanja et al., 2020). Gregurec et al. (2021) on the other hand, talk about sustainable business models during COVID-19 and while presenting a structured framework the authors address the importance of digital tools in this process, however, do not obsess over cybersecurity as would have been expected (Gregurec et al., 2021).

The emerging research gap from the literature evaluation highlights that integrated frameworks, such as SMEs could

be supported in managing operational as well as digital crises in parallel. In addition, the majority of research is focused on protection, as opposed to detection and recovery (Chidukwani et al., 2022; Dayour et al., 2023). The present study investigated the cybersecurity recovery strategies for SMEs in tourism but larger samples are needed to support the present work and subsequent research to validate the effectiveness of the strategies presented. This might include running pilot tests to pinpoint relevant detection and recovery measures particular to a key customer-facing sector, for example, the travel sector.

Methodology

Research Design

The present study utilized a mixed method to better understand cybersecurity risks in tourism SMEs in Cappadocia. This approach used qualitative and quantitative methods of data collection to provide an overview of particular cases, especially in tourism but also assess more general trends in cybersecurity behaviors and concerns (Dawadi et al., 2021).

Data Collection

Interviews: Eight semi-structured interviews were carried out in this study. The eight participants included cybersecurity experts, cybersecurity personnel, and stakeholders in the tourism industry. They were selected to obtain qualitative data on the concrete cybersecurity threats that affect SMEs in the tourism industry.

Questionnaire: The researchers of the current study designed a structured survey utilizing the Likert scale for 100 managers and employees of SMEs in the Cappadocia tourism sector. It assessed knowledge, level of readiness, and perceptions of cyber threats in various aspects including staff training, organizational measures in place, and perceived limitations. This method offered quantitative data for further understanding of the practices and threats in the field of cybersecurity across various businesses.

Sampling and Participants

Qualitative Study

The researchers of the current study utilized semi-structured interviews involving cybersecurity experts, Cybersecurity staff in Cappadocia, and local stakeholders in the tourism industry. The sample size was decided considering the inclusion of maximum different perspectives across different roles involved in cybersecurity practices in the tourism sector. The research team reached data saturation and found no new themes or ideas emerging to indicate data saturation, suggesting at least sufficient coverage of key cybersecurity challenges and perspectives in this context. This method provided an efficient summarization of the main cybersecurity issues and a thorough evaluation of their underlying concepts without redundancy.

Quantitative Study

The quantitative research involved identifying 100 participants who were selected based on the estimated size of the population of both employees and managers within tourism SMEs located in Cappadocia. Purposive sampling was used to ensure that participants had some understanding of cybersecurity practices, making them appropriate for the focus of the study. The sample size was an equilibrium between taking a representative sample and, at the same time, a feasible one that would provide enough information for a statistically relevant analysis. Furthermore, a sample size calculation using a 95% confidence level and 5% margin of error confirmed that 100 participants would provide reliable and generalizable insights into cybersecurity awareness, practices, and challenges within the population of tourism SMEs in Cappadocia.

Data Analysis

Both quantitative and qualitative data are analyzed using the Statistical Package for Social Sciences (SPSS) and NVivo software respectively to enable an analysis of cybersecurity practices that capture several layers.

Quantitative Analysis in SPSS: The collected survey data is analyzed quantitatively using IBM SPSS Statistics (version 26). The research applies descriptive and correlation analysis to determine the relationships between the level of awareness, the frequency of training, and the perception of readiness in the SMEs. The results outline some of the risks and, consequently, some of the deficiencies in terms of cybersecurity training and support.

Qualitative Thematic Analysis in NVivo: In analyzing the interview data collected from the respondents, NVivo (version 14) is used to analyze the data based on pre-identified major themes including cybersecurity awareness, challenges in implementing cybersecurity, and the resources required for effective cybersecurity implementation. Coding and categorization, presented in Appendix C, enabled the finding of recurring patterns that led to the offering of contextually relevant comprehension of the struggles that Cappadocia's tourism SMEs experience in attaining cybersecurity resilience.

RESULTS AND ANALYSIS

Qualitative Analysis of Cybersecurity Factors

This section of the study provides a thematic analysis of the interviews conducted with SMEs operating in Cappadocia's tourism industry. This work examines and categorizes the main issues concerning cybersecurity activities, attitudes, concerns, and requirements within this particular industry and its specific digital security requirements. These themes were deduced from the coding system utilizing Nvivo that had been adopted in the present study to pattern the data into codes that would reflect various issues of cybersecurity that were evident from the participants' responses.

Fig. 1 illustrates these themes and subthemes showing the link and interdependence of the data. This structured approach makes it possible to identify how tourism SMEs in Cappadocia perceive and manage cybersecurity and the positive aspects of internal and external risks in their digital processes.

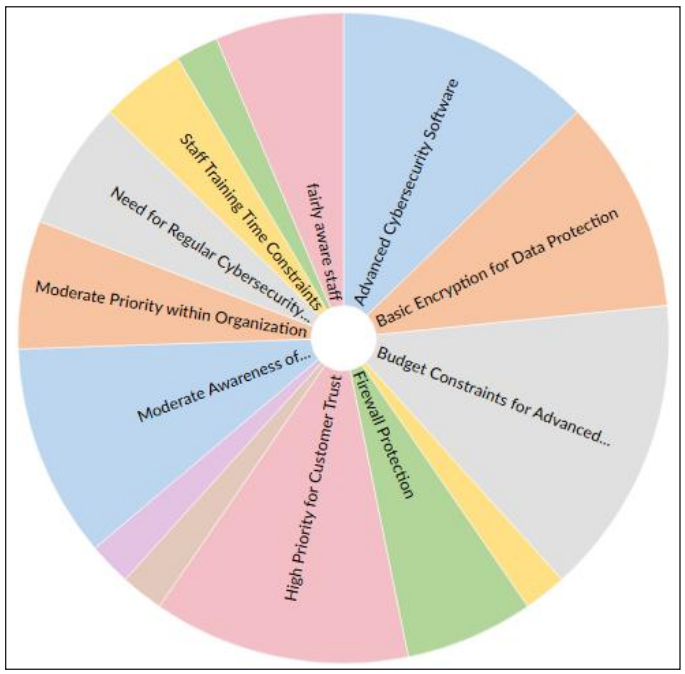


Fig. 1: Thematic Analysis of Cybersecurity Awareness, Measures, Challenges, and Resource Needs in Cappadocia's Tourism SMEs, Generated by Nvivo 14

Table 1 further illustrates the progression from initial codes to broader themes, providing insight into the primary cybersecurity factors affecting these businesses.

Table 1: Extraction of Key Themes from Coded Data on Cybersecurity in Cappadocia's Tourism SMEs

Theme	Codes
Cybersecurity Awareness	Low Awareness Among Staff Moderate Awareness of Industry-Specific Threats Need for Regular Cybersecurity Training
Cybersecurity Measures in Place	Basic Encryption for Data Protection Firewall Protection Limited Digital Tools for Security Transaction Security
Challenges in Implementing Cybersecurity	Budget Constraints for Advanced Security Staff Training Time Constraints Management or Customer Resistance
Importance of Cybersecurity for SMEs	High Priority for Customer Trust Moderate Priority within the Organization
Additional Resources Needed	Funding for Improved Security Tools Advanced Cybersecurity Software External Consultation and Support Enhanced Staff Training Programs

Theme 1: Cybersecurity Awareness

Some of the participants had a better understanding of the issues facing the Cappadocia tourism SME sector than others. It was found that although overall risk awareness was fairly good, threats that are specific to Cappadocia such as phishing scams to tourists or fake booking websites were sometimes ignored by the staff. For example, a cybersecurity officer remarked, *"Our team is fairly aware of cybersecurity basics, largely due to our regular training sessions. However, Cappadocia presents unique threats, such as fraudulent booking platforms mimicking our services during peak seasons, which poses a significant risk to our reputation and customer trust"*.

Some other respondents noted that it is difficult to retain a regional focus because the tourism business is seasonal in the area. An IT consultant explained, *"Staff have a basic understanding, but many don't realize how critical cybersecurity is in this region. Cyber threats here are often seasonal, with phishing schemes aligning with Cappadocia's peak tourism periods"*. This lack of awareness about region-specific threats highlights a critical gap in training, suggesting a need for focused educational programs that address Cappadocia-specific risks.

Theme 2: Cybersecurity Measures

The cybersecurity measures implemented by SMEs in Cappadocia's tourism industry primarily included basic protocols. These protocols mainly include SSL encryption and firewall protections. Several participants mentioned the use of secure payment gateways as a fundamental protective measure. For instance, the marketing director at Travel Atelier stated, *"We use secure payment gateways and encrypted channels to protect customer data. We're also vigilant about monitoring our social media presence, as fake profiles or promotions could easily deceive our clients"*.

However, respondents also noted limitations in their cybersecurity infrastructure, particularly due to budget constraints and high seasonal workloads. The customer service manager at Pupa Travel underlined these challenges, saying, *"A big challenge is the limited time we have for training during high seasons. It's hard to keep cybersecurity a top focus when we're so busy. Budget constraints also play a role; as advanced solutions can be costly"*. Another participant, a finance officer at Travel Atelier, added, *"Finding a balance between client convenience and security is a major challenge. Many clients prefer faster booking processes, so implementing additional verification steps is sometimes met with resistance"*.

Theme 3: Challenges in Implementing Cybersecurity

Challenges in implementing effective cybersecurity measures were a recurrent theme among Cappadocia's SMEs, with budget constraints, limited training time, and some resistance from management or customers cited as primary barriers. Budget limitations, in particular, were a challenge for many organizations. As a customer service manager at a travel agency noted, *"Advanced solutions can be costly, and during high season, our resources are stretched. It's hard to allocate extra funds to cybersecurity when there are other pressing expenses"*. This statement reflects the financial balancing act that many SMEs must navigate, especially when prioritizing daily operational needs over long-term cybersecurity investments.

Additionally, high seasonal demand impacted the availability of staff training, which left some employees underprepared for evolving threats. A participant commented, *"Training time is limited during our peak periods, so cybersecurity doesn't always get the attention it should. We're often focused on handling customer inquiries and bookings, and it's tough to fit in regular training sessions"*. Management and customer resistance to more rigorous security practices were another challenge. As the finance officer pointed out, *"Many clients prefer faster booking processes, so additional verification steps can be met with pushback"*. These constraints collectively hinder SMEs' ability to establish comprehensive cybersecurity protocols.

Theme 4: Importance of Cybersecurity for SMEs

For most participants, cybersecurity was a top priority, especially regarding customer trust and business reputation, though it varied in organizational focus. Cybersecurity's role in maintaining customer trust was frequently emphasized. As the operations manager explained, *"Protecting customer data is crucial, particularly in a popular destination like Cappadocia, where any data breach could severely impact our reputation"*. This reflects a high level of awareness of how cybersecurity directly relates to the brand's credibility.

Despite this, some participants indicated that cybersecurity is a moderate priority within their organizations, often competing with other operational needs. The tour coordinator remarked, *"While cybersecurity is important, we're primarily focused on delivering a quality travel experience. Balancing this with cybersecurity can be challenging, especially with limited resources"*. These differing levels of prioritization suggest that while SMEs understand the importance of cybersecurity in principle, practical implementation does not always align with this understanding due to competing organizational priorities.

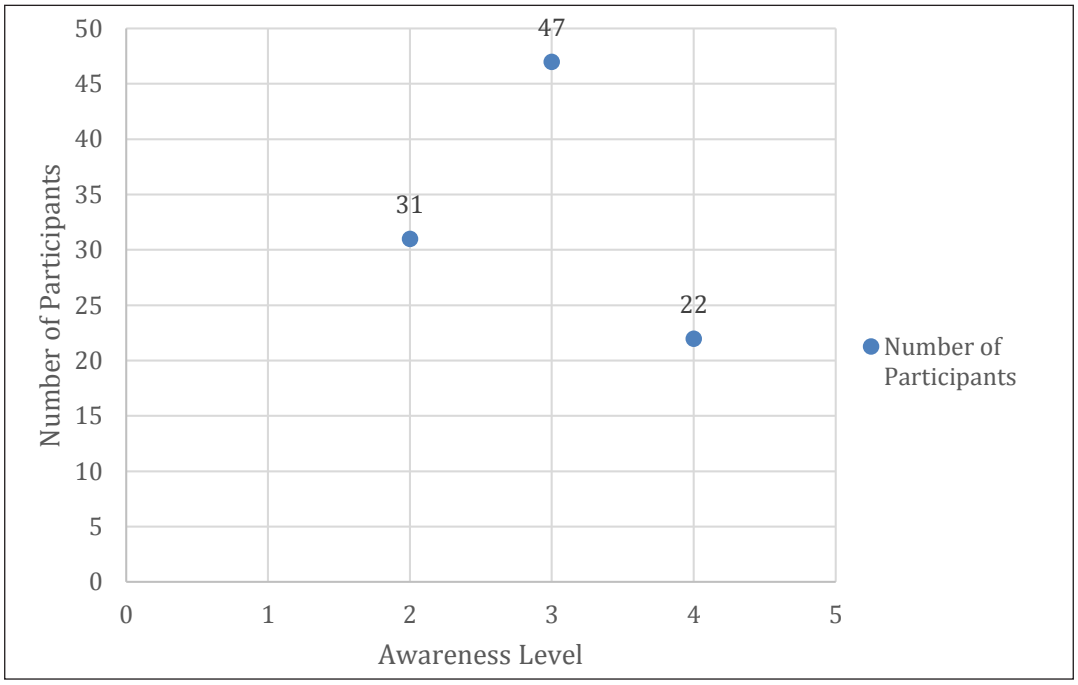
Theme 5: Additional Resources Needed

Participants consistently expressed the need for additional resources to strengthen cybersecurity, citing funding, advanced tools, external consultation, and enhanced staff training as critical requirements. A finance officer emphasized the need for financial support, stating, *"Funding would be incredibly helpful to acquire more advanced security tools. Many of these tools are beyond our budget but would make a big difference in our security setup"*. This indicates that current security measures are often limited by affordability, leaving potential vulnerabilities unaddressed.

The demand for external consultation and tailored training programs was also significant. An IT consultant explained, *"We would benefit from specialized training and support, particularly during peak seasons. Government-backed programs could help us keep up-to-date without stretching our resources too thin"*. This underscores the value of external support in augmenting internal cybersecurity capabilities, especially given the fast-evolving nature of digital threats in the tourism sector.

Quantitative Analysis of Cybersecurity Factors

Cybersecurity Awareness Levels Among SME Staff



Source: Generated by researchers.

Fig. 2: Distribution of Participants Based on Their Cybersecurity Awareness Level

The scatter plot of cybersecurity awareness levels reveals notable trends in the awareness among staff across Cappadocia's tourism SMEs. Awareness Level 3 with a basic understanding of cybersecurity threats was the largest group and consisted of 47 participants. Next is Awareness Level 2, in which the participants have a lower level of awareness, with 31 participants, and Awareness Level 4, with only 22 participants.

This distribution means that quite a large number of SME staff have only a fairly good or poor cybersecurity knowledge level. Such a low level of awareness might expose the organization to cyber risks as employees do not appreciate the importance of cybersecurity measures, or potential dangers. Affordability and access to cybersecurity training for SME staff are also important concerns Emerging from the survey results is a low number of participants with high awareness, which requires further training on awareness and knowledge of cybersecurity. Such initiatives could include creating awareness of certain cybersecurity threats that the tourism industry is likely to encounter, to train the employees on how best to handle them.

Descriptive Statistics

Table 2: Descriptive Statistics Showing the Mean, Standard Deviation, Minimum, and Maximum Values for Each Question (Q1-Q11)

Questions	N	Minimum	Maximum	Mean	Std. Deviation
Q1	100	2	4	2.91	.726
Q2	100	1	2	1.57	.498
Q3	100	1	3	1.91	.698

Questions	N	Minimum	Maximum	Mean	Std. Deviation
Q4	100	4	5	4.42	.496
Q5	100	4	5	4.36	.482
Q6	100	3	5	4.22	.760
Q7	100	4	5	4.47	.502
Q8	100	4	5	4.39	.490
Q9	100	4	5	4.38	.488
Q10	100	4	5	4.32	.469
Q11	100	4	5	4.39	.490
Valid N (listwise)	100				

Table 2 is a descriptive analysis of responses to all the questions (Q1-Q11) and gives the general distribution of the scaled responses reflecting the level of cybersecurity awareness, practice, problem, and importance. Some items with higher means including Q4 through Q11 indicate that the respondents have a positive attitude towards the importance of cybersecurity and the measures in place.

Correlations Between Key Variables

Table 3: Correlations Among Cybersecurity Awareness, Practices, and Challenges[1]

Dimension	Variables		Q1: General Awareness	Q2: Region-Specific Awareness	Q3: Sufficiency of Measures	Q4: Frequency of Updates
Awareness	*General Awareness (Q1)*	Pearson Correlation	1	.171	.024	.078
		Sig. (2-tailed)		.088	.815	.441
		N	100	100	100	100
	Region-Specific Awareness (Q2)	Pearson Correlation	.171	1	.266**	-.243*
		Sig. (2-tailed)	.088		.008	.015
		N	100	100	100	100
Perceived Sufficiency	*Sufficiency of Measures (Q3)*	Pearson Correlation	.024	.266**	1	-.298**
		Sig. (2-tailed)	.815	.008		.003
		N	100	100	100	100
Practice Updates	*Frequency of Updates (Q4)*	Pearson Correlation	.078	-.243*	-.298**	1
		Sig. (2-tailed)	.441	.015	.003	
		N	100	100	100	100

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

[1]Q1-Q4 represent different cybersecurity dimensions. The Pearson Correlation values indicate the strength of relationships among these variables, where values with ** and * denote significance at the 0.01 and 0.05 levels, respectively.

Table 3 reveals the correlation matrix of such variables, the important observations of which are as follows: Q2 is moderately positively correlated with Q3 at 0.01 level of significance; this indicates that the respondents, who believe that the organization has a pretty good idea of region-specific threats, also perceive that the organization

has sufficient cybersecurity measures in place. On the other hand, a negative though moderate and significant correlation between Q2 and Q4 means that as the awareness of region-specific threats increases the perceived need for update practices decreases indicating respondent complacency.

Table 4: Correlations Among Financial, Temporal, and Resource Constraints[1]

Dimensions	Variables		Q7: Financial Challenges	Q8: Time Constraints	Q9: Importance of Cybersecurity	Q10: General Resource Needs	Q11: Region-Specific Resource Needs
Resource Constraints	*Financial Challenges (Q7)*	Pearson Correlation	1	.274**	.130	.170	.233*
		Sig. (2-tailed)		.006	.199	.091	.020
		N	100	100	100	100	100
	Time Constraints (Q8)	Pearson Correlation	.274**	1	.177	.067	.117
		Sig. (2-tailed)	.006		.079	.509	.245
		N	100	100	100	100	100
Cybersecurity Priority	*Importance of Cybersecurity (Q9)*	Pearson Correlation	.130	.177	1	.170	.134
		Sig. (2-tailed)	.199	.079		.092	.183
		N	100	100	100	100	100
Resource Needs	*General Resource Needs (Q10)*	Pearson Correlation	.170	.067	.170	1	.155
		Sig. (2-tailed)	.091	.509	.092		.124
		N	100	100	100	100	100
	Region-Specific Resource Needs (Q11)	Pearson Correlation	.233*	.117	.134	.155	1
		Sig. (2-tailed)	.020	.245	.183	.124	
		N	100	100	100	100	100

[1]**Q7-Q11** represent dimensions related to resource constraints and needs, as well as the importance of cybersecurity. Correlations significant at the 0.01 level are marked with ** and those significant at the 0.05 level with *.

Table 4 provides additional information on correlations, such as financial and resource-based issues. A moderate correlation between Q7 and Q8, Q7 and Q11 shows that the difficulties of financial limitation are closely related to other resources; thus, the organizations with limited budgets also suffer from region-specific resources and the lack of time for improving cybersecurity.

Regression Analysis on Predictors of Updating Practices

Table 5: Regression Model Summary for Predictors of Updating Practices (Q4)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.362[a]	.131	.104	.470	.131	4.836	3	96	.004

a. Predictors: (Constant), Q3, Q1, Q2.

Table 5 shows the regression analysis for updating practices (Q4) where R^2 is 0.131 depicting that 13.1 percent of the variability of updating practices is explained by Q1, Q2, and Q3. The F-change of 0.004 suggests that the model is useful in general even though some predictors are more significant than others.

Table 6: Coefficients for Predictors of Updating Practices

Predictor	Coefficient (B)	p-Value
Constant	4.832	< 0.001
Q1 (General Awareness)	0.080	0.226
Q2 (Region-Specific Awareness)	-0.197	0.052
Q3 (Sufficiency of Measures)	-0.177	0.013

The coefficients for predictors of updating practices are shown in Table 6. In Q3 (sufficiency of measures), participants perceiving their cybersecurity measures to be sufficient offered a significantly (B = -0.177, p = 0.013) lower response to the updates item, implying that perceived sufficiency of cybersecurity measures leads to reduced continuing vigilance. However, Q1 and Q2 in the model demonstrate no effect on Q4, meaning that general and region-specific awareness does not have a strong effect regarding the frequency of updating practices in this sample.

Table 7: Regression Model Summary for Predictors of Cybersecurity Importance (Q9) Regression Model Summary for Predictors of Cybersecurity Importance (Q9)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	0.246	0.060	0.021	0.191	0.060	1.526	4	95	0.201

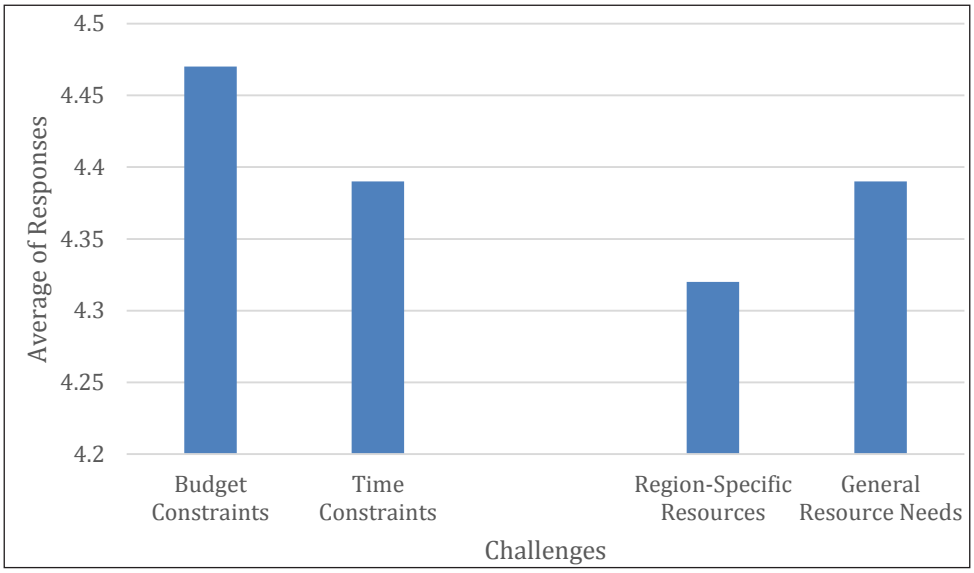
a. Predictors: (Constant), Q3, Q1, Q2.

Table 7 shows the regression model for the importance of cybersecurity (Q9); it has a computational R^2 equal to 0.060, which means that only 6% of the variation in cybersecurity importance is addressed by the predictors Q7, Q8, Q10, and Q11. This low R^2 coupled with an F-change that is not significant on 0.201 means that these predictors have little or no effect on the perception of the importance of cybersecurity in this model.

Table 8: Coefficients for Predictors of Cybersecurity Importance (Q9)

Predictor	Coefficient (B)	p-Value
Constant	3.842	< 0.001
Q7 (Financial Challenges)	-0.192	0.044
Q8 (Time Constraints)	-0.072	0.456
Q10 (General Resources Need)	0.103	0.280
Q11 (Region-Specific Resources Need)	-0.087	0.339

Last of all, Table 8 presents the results of regression coefficients for variables assessing cybersecurity importance. In particular, Q7 (financial issues) is the only predictor to reach statistical significance with a nearly negligible negative impact on the perceived importance of cybersecurity (B = - 0.192, p = 0.044). The other predictors, Q8, Q10, and Q11 do not influence the importance of cybersecurity, further affirming our argument that resources-based challenges alone do not powerfully point to an organization's perceived worth of cybersecurity.



Source: Generated by researchers.

Fig. 3: Cybersecurity Implementation Challenges

The main issues revealed by SMEs in Cappadocia in terms of cybersecurity implementation are shown in Fig. 3. Each of the challenges is divided into sub-topics of budgets, time, general requirements, and region requirements. In all the SMEs, budget restraints and time were the most reported challenges followed by the availability of general and regional resources.

Time and cost become key issues as the study indicates that SMEs are unlikely to afford quality cybersecurity solutions due to financial constraints. Such a limitation might compromise the efforts to invest in better software, training, or modern cybersecurity systems. Another important factor is time issues suggesting that SMEs might not have adequate staff or time to dedicate to constant cybersecurity checks and upgrades.

DISCUSSION

The findings show that Cappadocia's tourism SMEs have different levels of cybersecurity consciousness, and the seasonal-specific threats are a huge threat (Carías et al., 2020). For instance, although, they understand the basic issues to do with cybersecurity, the seasonal nature of these threats, for example, the phishing scams targeting tourists when they are visiting this area, these SMEs are always vulnerable (See Appendix B). According to Wilson et al. (2022), while SMEs are aware of cyber risks, the extent of protection remains relatively low because the actual level of protection does not match the perceived level of risk. Chidukwani et al. (2022) also emphasize the need for a holistic approach to cybersecurity, not only at the detection and recovery phase but also at other stages (Fernandez de Arroyabe et al., 2023). Especially for SMEs that are operating in the tourism sector, it might be during the low season that companies become vulnerable to phishing and social engineering scams, which aligns with Alkhalil et al.'s (2021) findings on how frequent customer interactions exacerbate vulnerability.

The levels of security implemented by the SMEs in Cappadocia were considered primitive and featured only mere encryption and firewalls. To a point made by the participants, inadequate finances and busy schedules during the busy seasons make it difficult to put in place enhanced protective measures. This limitation can be parallelled with Florido-Benítez (2024) and Dayour et al. (2023), who noted that despite the importance of digital readiness for competitive advantage in the tourism industry the lack of adequate security measures causes a significant threat to trust and operational issues. The challenges hindering the SMEs in terms of financial and operational resources to invest in proper and secure cyber systems are also supported by Kraj et al. (2022) who pointed out that the same situation explains the barriers that confront the Czech SMEs in balancing their current operational requirements against future security enhancements.

Difficulties in implementing cybersecurity were fairly large; the problems were the budget, little time for training employees, and some managers and customers resisting cybersecurity measures (Benz & Chatterjee, 2020). This finding is in line with Kukanja et al. (2020) and Gregurec et al. (2021) who pointed out that during crisis management

situations such as the current COVID-19 outbreak, the SMEs focused on other operational segments, consequently neglecting cyber risk management as a crucial segment to invest in. A similar constraint is also discussed by Parn and Edwards (2019) who argue that industries with critical assets, such as tourism, require a dynamic model that considers physical and cyber threats management.

Regarding cybersecurity, there was an understanding of its necessity from the participants, especially in terms of customer trust and reputation but its importance could interfere with operational concerns (Dias et al., 2022). This is in line with research that posits that even as SMEs in sectors such as tourism acknowledge that cybersecurity is useful in developing customer trust (Florido-Benítez, 2024; Wilson et al., 2023), financial constraints prevent them from implementing elaborate comprehensive cybersecurity solutions.

In the end, needs for additional resources required for improving cybersecurity measures were determined such as financial resources, improved software, external advice, and staff training (Zwilling et al., 2022). The condition confirms the hypotheses presented by Dayour et al. (2023) and Kraj et al. (2022) on external programs relevant to government and industry for SMEs' digital transformation. Lack of access to such extra resources keeps tourism SMEs endangered especially in such areas as Cappadocia where repetitive turnover of tourists increases their exposure to different digital threats (Civelek et al., 2023).

IMPLICATIONS

The study results presented in this paper outline several key directives that affect the cybersecurity status of SMEs in Cappadocia's tourism sector. The research indicates that with targeted cybersecurity awareness programs by regions of operation, SME tourism firms stand to gain due to an increased understanding of the different forms of phishing and social engineering that proliferate during the typical tourism seasons.

Strengthening Cybersecurity Policies and Training

From the literature and the findings of the current study, it can be inferred that within the tourism and hotel industry, the management should adopt clear internal policies and ensure constant training of the staff on Internet and database security to minimize vulnerability to cyber threats (Dhande, 2024; Maulana et al., 2022). The current study underlines the importance of the effective record of modern and extensive risks that can be useful for systematic evaluation of the severity in tourism organizations (Fernandez de Arroyabe et al., 2023). The study supports these recommendations, as our results showed that a majority of SMEs in Cappadocia have low levels of cybersecurity knowledge and protection. It is also suggested that the training programs aimed at specific regional threats: in this case, phishing attacks that occur before the tourist season, would help to improve the overall security system (Dhande, 2024; Fernandez de Arroyabe et al., 2023). Moreover, it means that the employees would be keen to the new threats arising within a year and be ready to embrace the necessary measures to avoid such threats.

Aligning with National Cybersecurity Frameworks

According to Liszkowska's (2024) analysis of Turkey's national cybersecurity policies, its goals are to build up cyber defense and bring it into line with the international level. However, these frameworks at the moment do not take into consideration any sector requirements within tourism (Carías et al., 2020; Liszkowska, 2024). If Turkey fully consolidates the industry standards with the national goals of cybersecurity, the tourism industry can optimize the available sources and knowledge to prevent sophisticated cyber risks. Furthermore, Akyesilmen (2022) considers certain aspects of the national cybersecurity policies and strategies in Turkey as strong in legal and organizational terms, but, weak in technical terms. Based on this study, it is recommended that those who seek to strengthen the technical competence of tourism SMEs, in such areas as data security management and real-time threat identification, might do well to offer SMEs affordable and sustainable cybersecurity solutions (Akyeşilmen, 2022).

Emphasizing Cybersecurity as a Policy Priority

Bearing in mind that customer trust is a critical asset in the tourism industry and data security is a critical component of the tourism business strategy, it can be concluded that cybersecurity should be defined as one of the major policy priorities. As for the role of institutional arrangements, Aguinis et al. (2023) write that public policies that arise in response to market failures are at the heart of industry advancements. Such perspective resonates with our findings, which suggest that due to the resource deficits and a lack of cybersecurity expertise SMEs in the Turkish tourism sector struggle to adopt proper cybersecurity measures (Aguinis et al., 2023; Seow et al., 2024). An example of government response could be to establish grant or tax credit programs designed to get tourism-related businesses to start buying

cybersecurity. Further, it is equally possible to integrate other sectors, particularly with cybersecurity firms, to help SMEs develop better protection systems meeting their precise requirements (Aguinis et al., 2023; Seow et al., 2024).

CONCLUSION

This research underscored the challenges of cybersecurity for SMEs in the tourism industry of Cappadocia, the digitalization, and seasonal fluctuations contributing to these challenges. Although these SMEs understand the relevance of cybersecurity in preserving customer confidence and organizational efficiency, financial constraints, lack of training, and the sheer pressure of business activity hamper optimal execution. Based on the literature about SMEs and cybersecurity measures, this research elucidates that tourism-oriented SMEs have extremely high potential to leverage the help from government cybersecurity programs, organizational training, and development, as well as affordable and efficient innovative IT security products and services to support. It is crucial to meet these needs to help Cappadocia's tourism SMEs become digitally sustainable and capable of operating in a digital and otherwise high-risk environment.

REFERENCES

Aguinis, H., Kraus, S., Poček, J., Meyer, N., & Jensen, S. H. (2023). The why, how, and what of public policy implications of tourism and hospitality research. *Tourism Management*, *97*, 104720.

Akyeşilmen, N. (2022). Türkiye in the global cybersecurity arena. *Insight Turkey*, *24*(3), 109–134.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

Ardıç Yetiş, Ş., Deniz, G., Aydın, Ş., & Dalkılıç, F. (2022). An evaluation on the problems and solutions of cappadocia regional tourism.

Arroyabe, M. F., Arranz, C. F., de Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges. *Technological Forecasting and Social Change*, *199*, 123051.

Asgary, A., & Ozdemir, A. I. (2020). Global risks and tourism industry in Turkey. *Quality & Quantity*, *54*(5), 1513–1536.

Asgary, A., Ozdemir, A. I., & Özyürek, H. (2020). Small and medium enterprises and global risks: Evidence from manufacturing SMEs in Turkey. *International Journal of Disaster Risk Science*, *11*, 59–73.

Aydın, Ş., & Akpınar, A. (2023). Faith tourism potential of Cappadocia region. *Request & Demand Address*, 343.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540.

Bouramdane, A.-A. (2023). Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*, *3*(4), 662–705.

Büyükkuru, M., & Yılmaz, İ. (2022). Determining the development level of Cappadocia tourism.

Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2021). Cyber resilience self-assessment tool (CR-SAT) for SMEs. *IEEE Access*, *9*, 80741–80762.

Carías, J. F., Borges, M. R., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, *8*, 174200–174221.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, *10*, 85701–85719.

ÇİFTÇİ, F., & COŞKUN, İ. O. (2023). İktisat ve Turizm Politikası Kaymalarının Türkiye'de Turizm Arzına Etkilerinin Yapısal Kırılmalı Birim Kök Testleri ile Analizi (Examining the Effects of Economic and Tourism Policy Shifts on Tourism Supply in Turkiye Using Structural Break Unit Root Test. *Journal of Tourism & Gastronomy Studies*, *11*(3), 2114–2135.

Civelek, M., Krajčík, V., & Ključnikov, A. (2023). The impacts of dynamic capabilities on SMEs' digital transformation process: The resource-based view perspective. *Oeconomia Copernicana*, *14*(4), 1367–1392.

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: A discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education*, *2*(2), 25–36.

Dayour, F., Adongo, S., & Kosoe, E. A. (2023). The boon and bane of ICT services to small and medium-sized tourism and hospitality enterprises (SMTHEs) in northern Ghana. *Small Enterprise Research*, *30*(2), 255–273.

De Pascale, A., Bixio, R., & Caloi, V. (2023). Rupestrian cultures of Turkey: Reflections on the analysis and classification of a fragile heritage. *di Firenze*, 17.

Dhande, K. R. (2024). Fourth industrial revolution and the role of cyber security: Technologies on the travel and tourism industry and more specifically cyber security in travel tourism. In *Corporate Cybersecurity in the*

Aviation, Tourism, and Hospitality Sector (pp. 241–257). IGI Global.

Dias, Á. L., Cunha, I., Pereira, L., Costa, R. L., & Gonçalves, R. (2022). Revisiting small-and medium-sized enterprises' innovation and resilience during COVID-19: The tourism sector. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(1), 11.

Eldem, T. (2020). The governance of Turkey's cyberspace: Between cyber security and information security. *International Journal of Public Administration*, *43*(5), 452–465.

Fernandez de Arroyabe, J. C., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. (2023). Cybersecurity resilience in SMEs. A machine learning approach. *Journal of Computer Information Systems*, 1–17.

Florido-Benítez, L. (2024). The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities. *Smart Cities*, *7*(1), 475-495.

Gregurec, I., Tomičić Furjan, M., & Tomičić-Pupek, K. (2021). The impact of COVID-19 on sustainable business models in SMEs. *Sustainability*, *13*(3), 1098.

Günden, Y., & Günden, B. (2022). An innovative culture route proposal in destination management of Cappadocia region. *Revista Rosa dos Ventos-Turismo e Hospitalidade*, *14*(3).

Irani, F., Athari, S. A., & Hadood, A. A. A. (2022). The impacts of country risk, global economic policy uncertainty, and macroeconomic factors on the Turkish tourism industry. *International Journal of Hospitality & Tourism Administration*, *23*(6), 1242–1265.

Jiang, Y., Ritchie, B. W., & Verreynne, M. L. (2019). Building tourism organizational resilience to crises and disasters: A dynamic capabilities view. *International Journal of Tourism Research*, *21*(6), 882–900.

KRAJČÍK, V. (2021). The readiness of small and medium-sized enterprises (SMEs) for the digitalization of industry: Evidence from the Czech Republic. *Acta Montanistica Slovaca*, *26*(4).

Kumar, G., Sharma, D., Bhardwaj, B., & Chand, M. (2025). Seventeen years of International Journal of Hospitality and Tourism Systems: A bibliometric and thematic analysis. *International Journal of Hospitality & Tourism Systems, 18*(2).

Kukanja, M., Planinc, T., & Sikošek, M. (2020). Crisis management practices in tourism SMEs during the COVID-19 pandemic. *Organizacija*, *53*(4), 346–361.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186.

Liszkowska, D. (2024). Türkey's cybersecurity policy framework. *Cybersecurity and Law*, *11*(1), 79–91.

Maulana, A., Oktaviyanti, D., Wahyuni, D., Sasono, N., & Sakti, G. (2022). Implikasi Kebijakan Atas Terbitnya Travel & Tourism Development Index 2021 Terhadap Upaya Peningkatan Daya Saing Kepariwisataan Indonesia di Pasar Global. *Jurnal Kepariwisataan Indonesia: Jurnal Penelitian dan Pengembangan Kepariwisataan Indonesia*, *16*(2), 149–162.

Özen, İ. A. (2020). Internet of things in tourism: A proposal of the information system for Cappadocia hot-air ballooning. In *Handbook of Research on Smart Technology Applications in the Tourism Industry* (pp. 131-154). IGI Global.

Öztürk Büke, F. G. (2023). Tourism-led adaptive reuse of the built vernacular heritage: A critical assessment of the transformation of historic neighbourhoods in Cappadocia, Turkey. *The Historic Environment: Policy & Practice*, *14*(4), 474–497.

Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management*, *26*(2), 245–266.

Rastegar, R., Seyfi, S., & Shahi, T. (2023). Tourism SMEs' resilience strategies amidst the COVID-19 crisis: The story of survival. *Tourism Recreation Research*, 1–7.

Seow, A. N., Choong, Y. O., Low, M. P., Ismail, N. H., & Choong, C. K. (2024). Building tourism SMEs' business resilience through adaptive capability, supply chain collaboration and strategic human resource. *Journal of Contingencies and Crisis Management*, *32*(2), e12564.

Tariq, M. U. (2024). Cybersecurity risk assessment models and theories in the travel and tourism industry. In *Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector* (pp. 1–17). IGI Global.

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It won't happen to me: Surveying SME attitudes to cyber-security. *Journal of Computer Information Systems*, *63*(2), 397–409.

Yağcı, K., Akçay, S., Efendi, M., & Öztürk, H. M. (2020). Information security awareness in tourism enterprises: Case of Turkish manager opinions. In *Industrial and Managerial Solutions for Tourism Enterprises* (pp. 251–267). IGI Global.

Yetiş, Ş. A., Deniz, G., Aydın, Ş., & Yılmaz, F. D. (2022). An evaluation on the problems and solutions of Cappadocia regional tourism. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi*, *10*(1), 71–83.

Yigit Ozkan, B., & Spruit, M. (2023). Adaptable security maturity assessment and standardization for digital SMEs. *Journal of Computer Information Systems*, *63*(4), 965-987.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97.