DOI: https://doi.org/10.18778/0867-5856.2026.16 e-ISSN 2080-6922, ISSN 0867-5856

COPE Member since 2019 JM14487

Turyzm/Tourism
2026, *36*(2)

The role of employees as a key factor in hotel cybersecurity

Blaž Markelj[a], Ajda Šulc[b], Janez Mekinc[c, *]

[a] University of Maribor (Maribor, Slovenia), Faculty of Criminal Justice and Security; https://orcid.org/0009-0005-2951-8086; e-mail: blaz.markelj@um.si
[b] University of Maribor (Maribor, Slovenia), Faculty of Criminal Justice and Security; https://orcid.org/0000-0002-3562-402X; e-mail: ajda.sulc@um.si
[c] University of Primorska (Portorož, Slovenia), Faculty of Tourism Studies Turistica; https://orcid.org/0000-0001-7288-4982; e-mail: janez.mekinc@fts.upr.si
[*] Corresponding author.

Acknowledgements
The research was funded by the University of Rijeka, Faculty of Tourism and Hospitality Management, within the framework of the project ZIP-FMTU-015-11-2022.

How to cite (APA style): Markelj, B., Šulc, A., & Mekinc, J. (2026). The role of employees as a key factor in hotel cybersecurity. *Turyzm/Tourism, 36*(2), 7–18. https://doi.org/10.18778/0867-5856.2026.16

ABSTRACT

This study examines behavioral, organizational and psychological factors influencing hotel employees' reporting of cybersecurity incidents, focusing on trust relationships and technical knowledge. The aim was to determine how trust in internal IT staff versus external institutions is associated with reporting intentions and how employees' skills shape responses to cyber threats. A quantitative survey of 143 hotel employees was conducted, followed by statistical analyses, including paired *t*-tests and association-based regression models, to examine differences in reporting likelihood across channels. Results show that employees place the highest trust in internal IT experts, viewing them as the primary contact, while willingness to report to external institutions remains low, likely due to limited awareness or perceived procedural complexity. A paradox emerged: technically skilled employees, despite recognizing more threats, are less inclined to report incidents externally, often due to overconfidence, whereas less skilled employees exhibit greater caution and higher reporting rates. Employees trust basic security measures more than advanced tools, which are seen as complex. Findings underscore the need for targeted training, simplified reporting protocols, and stronger collaboration with external security actors, framing cybersecurity as a strategic element of hotel risk management.

KEYWORDS

cybersecurity, hospitality, security culture, employees, incident reporting

ARTICLE INFORMATION DETAILS

Received:
8 January 2026
Accepted:
18 May 2026
Published:
17 September 2026

Funding information: University of Rijeka, Faculty of Tourism and Hotel Management – Project ZIP-FMTU-015-11-2022. **Conflicts of interests:** None. **Ethical considerations:** The Authors assure of no violations of publication ethics and take full responsibility for the content of the publication. **The percentage share of the Author in the preparation of the work is:** B.M. 30%, A.Š. 30%, J.M. 40%. **Declaration regarding the use of GAI tools:** They used ChatGPT for language editing and improving the clarity of the manuscript. The tool was used to improve grammar, wording, and readability of selected sections of the text. The Authors then carried out a thorough and critical review of the text, with particular attention to potential false, incomplete, or biased information, possible plagiarism or lack of proper/accurate authorship attribution, and revised it accordingly.

1. Introduction

Digitalisation has fundamentally transformed the tourism and hospitality industry, increasing its reliance on interconnected information systems and data-driven service delivery, but also increased exposure to cybersecurity risks. As hotels routinely process large volumes of personal and financial data, cybersecurity has become a strategic organisational concern rather than merely a technical issue (Casais & Ferreira, 2023).

International policy-oriented analyses have long emphasised that human error and organisational processes represent critical vulnerabilities in cybersecurity risk management, indicating that technical safeguards alone are insufficient to ensure effective protection (Organisation for Economic Co-operation and Development [OECD], 2017). Although industry reports indicate that tourism and hospitality are among the sectors most exposed to cyber threats, recent academic research suggests these risks cannot be fully understood from a purely technological perspective. Contemporary hospitality and tourism literature increasingly emphasises that cyber resilience is shaped by the interaction of technological safeguards, organisational practices and employee behaviour (Alonso-Almeida & Giglio, 2024; Florido-Benítez, 2024, 2025). Hotels are particularly vulnerable to cybersecurity incidents due to their intensive use of digital systems and handling of sensitive data (Pipyros & Liasidou, 2025).

Recent studies highlight a shift from purely technological protection measures towards human-centred and organisational perspectives on cybersecurity. In this context, employees are increasingly recognised as a critical line of defence in cybersecurity incident response, as behavioural factors such as risk perception and trust significantly influence the effectiveness of cybersecurity practices (Bishop et al., 2025). This shift reflects a broader recognition that human error, delayed reactions and inadequate reporting frequently contribute to the escalation of cybersecurity incidents in service organisations.

From a theoretical perspective, employee cybersecurity behaviour has increasingly been examined through motivation-based frameworks, particularly protection motivation theory (PMT). Protection motivation theory explains protective behaviour as the result of threat appraisal (e.g., perceived severity and vulnerability) and coping appraisal (e.g., response efficacy, self-efficacy and trust in protective measures). Recent empirical studies confirm the applicability of PMT in organisational and service contexts, including tourism and hospitality, where employees operate under constant digital exposure and time pressure (de Bruin & Mersinas, 2024; Ozturk, 2026). In contrast to alternative frameworks frequently used in information systems research – such as the theory of planned behavior (TPB), the technology acceptance model (TAM), or deterrence theory – which primarily explain intention formation, technology adoption or compliance driven by sanctions – PMT focuses specifically on how individuals assess threats and evaluate their capacity to cope with them. This makes PMT particularly suitable for analysing cybersecurity incident reporting behaviour, as reporting decisions inherently involve both threat appraisal and coping appraisal related to different reporting channels. Johnston and Warkentin (2010) extend this theoretical perspective by examining fear through the fear appeal model (FAM), which is conceptually derived from PMT. The FAM operationalises PMT in the context of information security by explaining how fear appeals embedded in organisational communication stimulate employees' threat and coping appraisals, ultimately shaping their security-related behavioural responses.

Despite the growing body of research on cybersecurity in the hospitality industry, most existing studies have focused on general security awareness and preventive behaviour. In contrast, cybersecurity incident reporting remains underexplored as a distinct behavioural outcome. Incident reporting involves not only recognising a threat but also deciding whether and to whom to report it. Such decisions are shaped by employees' prior experience with cyber threats, their knowledge of risks, and their trust in cybersecurity solutions and reporting institutions. Moreover, internal reporting channels and external actors – such as IT departments, national computer emergency response teams (CERTs), law enforcement agencies and regulators – serve fundamentally different roles and entail different perceived consequences, indicating that incident reporting cannot be treated as a uniform or purely technical response. National-level incident statistics further illustrate the operational relevance of CERT institutions for coordinated cyber incident response in the hospitality sector (National CERT [CERT.hr], 2025). Specifically, internal reporting to hotel IT/management primarily supports rapid operational containment and recovery, whereas external reporting triggers institution-specific processes: CERTs typically provide technical coordination and guidance, while law enforcement focuses on investigation and evidence, and regulators enforce compliance with incident notification obligations. These role differences imply that employees may evaluate reporting channels based on distinct perceived consequences and expected support.

Accordingly, this study addresses the underexplored problem of cybersecurity incident reporting among hotel employees by examining how their knowledge

of cyber threats, prior experience with incidents, and trust in cybersecurity solutions are associated with their willingness to report incidents through internal and external reporting channels. By adopting a theory-informed behavioural perspective, the study seeks to clarify the mechanisms shaping channel-specific reporting intentions in the hotel context and to provide practical insights for strengthening organisational incident response.

2. Literature review

The hospitality industry is increasingly reliant on digital systems and interconnected infrastructures. In particular, cybersecurity is becoming critical in relation to incident detection and reporting processes where employee behaviour plays a central role. While early research on cybersecurity in tourism and hospitality focused mainly on technical safeguards and system vulnerabilities, more recent studies emphasise that effective cybersecurity management requires a holistic approach combining technical, organisational and behavioural dimensions (Florido-Benítez, 2025; Rid & Buchanan, 2015). Hotels routinely process large volumes of sensitive personal and financial data through reservation systems, loyalty programmes, mobile applications and payment platforms. This makes hotels particularly vulnerable to cyber threats (Chen & Jai, 2019; Pipyros & Liasidou, 2025). Consequently, cyber incidents in the hospitality industry often result not only from technical shortcomings but also from human error, delayed responses and lack of internal coordination.

Although technological solutions such as encryption, surveillance systems and access control are necessary components of cybersecurity strategies, they are not sufficient on their own. Empirical evidence increasingly shows that organisational readiness and employee behaviour play a decisive role in reducing cyber risks and limiting the consequences of security incidents (Fragnière & Yagci, 2021; Yallop et al., 2023). This shift has fuelled growing scholarly interest in behavioural and organisational theories that explain employee decision-making related to cybersecurity. While the hospitality literature increasingly recognises the importance of the human factor, much research remains descriptive and lacks a clear theoretical framework to explain why employees choose to engage in protective or risky cyber behaviours, especially regarding incident response and reporting. In particular, limited attention has been paid to how employees decide whether to report incidents through different reporting channels, such as internal organisational structures versus external institutions.

Protection motivation theory provides a theoretical basis for analysing individual cybersecurity behaviour and has been widely applied in information security research to explain protective actions (de Bruin & Mersinas, 2024; Maddux & Rogers, 1983; Rogers, 1975). According to PMT, protective behaviour is shaped by two cognitive processes: threat appraisal and coping appraisal. Threat appraisal reflects perceived severity and vulnerability and, in a cybersecurity context, is influenced by employees' knowledge of threats and prior experience with cyber incidents. Coping appraisal reflects response efficacy and self-efficacy, as well as contextual factors such as trust in security solutions and organisational support (de Bruin & Mersinas, 2024). In hospitality settings, where employees play a key role in identifying and responding to cyber risks, these appraisals are particularly relevant (Ozturk, 2026). Accordingly, this study conceptualises cybersecurity incident reporting as a protective behaviour influenced by both threat and coping appraisals.

Recent empirical studies confirm the applicability of PMT in organisational and service settings, including tourism and hospitality, where employees work under time pressure, face frequent interruptions and are constantly exposed to digital media (Bishop et al., 2025). Research based on PMT suggests that employees are more likely to adopt protective cyber behaviours when they perceive threats as serious and believe that reporting or responding to incidents will be effective and supported by the organisation. However, these studies rarely examine incident reporting behaviour as a distinct outcome, particularly in terms of differences between internal and external reporting channels. Despite the relevance of PMT, this theory has mainly been used to study general cyber compliance and preventive behaviours, and its potential to explain cyber incident reporting behaviour, especially through different reporting channels, remains underexplored in hospitality research. In addition to individual cognitive processes, employee behaviour is embedded in an organisational context that shapes norms, expectations and perceived consequences. The concept of cybersecurity climate refers to shared perceptions of the importance of cybersecurity, leadership commitment, training and reporting practices within an organisation (Arcuri et al., 2020; Chang & Lin, 2007; Kraemer et al., 2009). It reflects how employees interpret organisational expectations related to information security and the extent to which secure behaviour is supported, encouraged, and reinforced within the organisation. Research consistently shows that a strong security culture increases employees' awareness of cyber threats and their willingness to take protective measures, including reporting suspicious activity (Arcuri et al., 2020; Srivastava et al., 2022). Conversely, a weak security culture, unclear reporting procedures,

and fear of negative consequences discourage employees from reporting incidents, even when they recognise threats. Nevertheless, prior studies often treat reporting behaviour as a general outcome, without distinguishing between different reporting channels or institutional contexts. In the hospitality environment, where operational priorities often focus on speed of service and guest satisfaction, reporting cyber incidents can be perceived as disruptive or risky. Employees may choose not to report incidents if they believe they can resolve them themselves or if they do not trust the reporting process (Fragnière & Yagci, 2021). These findings highlight the importance of organisational trust and perceived leadership support as key antecedents of reporting behaviour. However, existing studies predominantly focus on general cybersecurity behaviour or compliance, while relatively limited attention has been paid to channel-specific incident reporting behaviour, particularly in service-oriented contexts such as hospitality. Although previous studies confirm the link between security climate and general cyber behaviour, less is known about how security culture, together with individual perceptions (e.g. experience, trust), shapes reporting intentions, especially in the hotel environment.

Reporting cyber incidents is fundamentally different from general security compliance or preventive behaviour. Reporting involves acknowledging a potential error, taking responsibility and initiating formal procedures that may have operational, legal or reputational consequences. Therefore, reporting decisions are influenced not only by perceived risk but also by institutional trust and perceived consequences (Srivastava et al., 2022). It is important to emphasise that reporting channels are not homogeneous. Internal reporting (e.g. to IT or management) is primarily intended to facilitate rapid response and limit damage. In contrast, external reporting to national CERTs, law enforcement or regulatory institutions involves different mandates, roles and contexts of intervention. These institutions vary in their focus on technical assistance, investigation or compliance, which can influence employees' willingness to report. Treating these institutions as equivalent reporting targets obscures important behavioural differences and reduces analytical precision. Employees' decisions about whom to report an incident to reflect their trust in the institutions, expectations of support, and perceived personal and organisational consequences. Despite this conceptual distinction, hospitality research rarely provides an empirically grounded analysis of how these channel-specific differences influence reporting behaviour. Hospitality research rarely distinguishes between internal and external reporting channels or examines how employees' perceptions shape reporting behaviour across channels. In this study, reporting targets are therefore conceptualised as (a) internal operational response (hotel IT expert); (b) technical external coordination (national Computer Emergency Response Team and Information Systems Security Bureau); (c) service provider support (mobile operator/internet provider); and (d) legal-compliance pathways (law enforcement and the national data protection authority). This distinction informs the interpretation of channel-specific reporting likelihoods.

The synthesis of the aforementioned theoretical approaches suggests that the cyber incident reporting behaviour of hotel employees results from an interplay of individual cognitive judgements (as defined by PMT), organisational security climate, and institutional trust in reporting channels. Prior experience with cyber incidents and knowledge of threats influence threat judgement, while trust in security solutions and reporting procedures influences coping judgments and reporting intentions. Despite the growing interest in cybersecurity in the hospitality industry, existing research does not provide a sufficiently theoretically grounded analysis of incident reporting as a distinct, channel-specific behavioural outcome. In this context, this study specifically focuses on employees' incident reporting behaviour, addressing the gap between general cybersecurity awareness and actual reporting decisions across internal and external channels. To address this gap, this study uses PMT to examine how employees' experiences with cyber threats, their knowledge of risks, and trust in cybersecurity solutions relate to their willingness to report incidents to various institutions.

3. Method and sample

Between August 2023 and April 2024, a quantitative cross-sectional survey was conducted among employees of hotels operating in Croatia. Data were collected using an online questionnaire administered via the 1KA.si survey platform. The questionnaire consisted of 28 items addressing respondents' demographic characteristics, job-related variables, experience with cybersecurity incidents, knowledge of cyber threats, trust in cybersecurity solutions, and incident reporting behaviour. The survey design allows for the examination of relationships among variables at a single point in time but does not support causal inference.

Due to the limited accessibility of the target population and the absence of a comprehensive sampling frame for hotel employees, a non-random convenience sampling approach was employed. Hotel management teams with whom prior cooperation had been established

were contacted by email and asked to forward the survey link to their employees. This approach is consistent with exploratory research designs in hospitality settings, where access to employees is often mediated by organisational gatekeepers. Accordingly, the findings are interpreted as indicative of statistically meaningful associations among variables rather than as representative or causal estimates applicable to the broader population of hotel employees.

A total of 214 respondents took part in the survey, of whom 143 provided complete responses suitable for analysis. Table 1 presents the demographic characteristics of the final sample. The sample included a higher proportion of male respondents (59.7%) than female respondents (40.3%). Most participants were between 26 and 44 years of age, and the majority held at least a first- or second-cycle Bologna degree.

Table 1. Proportion of valid answers by demographic characteristics of respondents

Demographic category	Group	Proportion (%)
Gender	Woman	40.3
	Man	59.7
Age	<20 years	7.5
	21–25 years	12.1
	26–34 years	29.0
	35–44 years	30.8
	45–54 years	14.0
	Older	6.5
Education	Secondary school	22.8
	Bologna level 1	30.1
	Bologna level 2	40.8
	Bologna level 3	6.3

Source: authors.

Respondents occupied a range of job positions within their hotels. The largest groups were middle management (26.4%), managerial positions (16.5%), administration (13.2%), sales (12.7%) and service-related roles (11.8%). Smaller proportions were employed in technical positions (9.4%), executive roles (5.7%) or other functions (4.2%). The hotels represented in the sample were located primarily in the Kvarner region (51.9%), followed by Dalmatia (19.2%), Continental Croatia (17.8%), and Istria (11.1%). Nearly half of the respondents worked in medium-sized hotels (51–200 rooms), with fewer employed in large hotels (more than 200 rooms) or small (5–50 rooms). Most respondents were employed in hotels belonging to national hotel chains (54.1%), while fewer worked in independent hotels (26.8%) or international chains (19.0%).

Regarding work-related technology use, most respondents reported using devices owned by their employer. Hotel-owned desktop computers were used by 75.4% of respondents, smartphones by 73.3%, and laptops by 65.2%. Tablets were less common, with a majority of respondents (56.2%) reporting the use of personally owned devices. These contextual characteristics provide relevant background for interpreting employees' exposure to digital systems and cybersecurity-related practices but are not treated as causal determinants of reporting behaviour.

3.1. Research hypotheses

Drawing on protection motivation theory and prior research on cybersecurity behaviour and incident reporting, this study formulates the following hypotheses to guide the empirical analysis. Given the cross-sectional and exploratory nature of the research design, the hypotheses are framed in terms of expected associations rather than causal relationships.

H_1: Hotel employees are more likely to report cybersecurity incidents to internal IT experts or management than to external reporting channels.

H_2: Employees' knowledge of cyber threats and experience with cybersecurity incidents are associated with their willingness to report incidents to external institutions.

H_{2a}: Greater knowledge of cyber threats is associated with a lower likelihood of reporting cybersecurity incidents to external institutions.

H_{2b}: Higher trust in cybersecurity solutions beyond basic authentication mechanisms is associated with a higher likelihood of reporting cybersecurity incidents to external institutions.

Consistent with the institutional differentiation discussed above, these associations are expected to be more pronounced for external technical and legal-compliance reporting channels than for internal organisational reporting.

4. Research and results

4.1. Variables

We measured the likelihood of reporting an information security incident with two separate questions: one specifically for incidents on computers and one for incidents on smartphones. Respondents rated the likelihood of reporting for each of the seven institutions or individuals on a 5-point scale, which we consider to be numeric for the purpose of the testing. Table 2 shows

Table 2. Probability of reporting a cyber incident – by device and type of institution

IT expert in the company	4.0	1.2	−1.0	−0.2	4.0	1.2	−1.1	0.2
Mobile operator	3.0	1.3	0.0	−0.9	3.0	1.2	0.1	−0.6
AZOP	2.9	1.3	−0.1	−1.0	2.8	1.3	0.1	−1.1
Internet provider	2.9	1.2	0.1	−0.6	2.8	1.2	0.2	−0.6
ISSB	2.8	1.3	−0.0	−1.0	2.8	1.3	0.1	−1.0
National CERT	2.8	1.3	0.1	−1.0	2.8	1.3	0.1	−0.9
Police	2.5	1.4	0.5	−1.1	2.4	1.3	0.6	−0.8

Note: *M* – mean; *SD* – standard deviation; AZOP – Agencija za zaštitu osobnih podataka (Croatian Personal Data Protection Agency); CERT – Computer Emergency Response Team; ISSB – Information Systems Security Board.

Source: authors.

the average values of the responses, their variability, and the coefficients of asymmetry and kurtosis. These show that all variables are approximately normally distributed. If respondents experienced a security incident on their computer or smartphone, they would be most likely to report it to the hotel's IT expert and less likely to their mobile operator, the Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka [AZOP]), and their internet provider. Respondents would be least likely to report an incident on either type of device to the police.

To improve analytical precision, the seven reporting targets are interpreted in terms of their institutional functions. Specifically, hotel IT experts represent an internal operational response channel; national CERT and ISSB represent technical coordination channels; mobile operators and internet providers represent service provider channels; and the police and AZOP represent legal-compliance channels. This classification is used in the interpretation of the reporting patterns reported in Table 2.

To test the first hypothesis, we performed paired *t*-tests comparing the probability of reporting an incident to an IT expert at a hotel and all other institutions, separately for incidents on computers and smartphones. For all pairs of variables, we obtained statistically significant differences between the means (all $p < 0.001$). Taken together, the results indicate that, within this sample, the probability of reporting a cybersecurity incident to an internal IT expert on both devices is statistically significantly higher than the probability of reporting to any other institution ($\alpha = 0.05$).

We measured threat awareness by listing nine categories and asking respondents to indicate whether they were aware of each threat. For the same categories, we then asked them whether they had ever been exposed to any of these threats. The frequencies of the selected responses are shown in Table 3. The most common threats people are familiar with are malware infection and loss of access to data, which were also the most commonly experienced types of threats. The fewest people were familiar with distributed denial-of-service (DDoS) attacks, while theft of business-critical data and intrusion into information systems were the least common types to happen to respondents.

Table 3. Familiarity and experience with various threats to information and communication systems (ICSs)

Type of threat	Familiarity (*n*)	Threat experienced (*n*)
Malware infection	113	62
Loss of access to data	110	64
Phishing	106	60
Information system intrusion	98	24
Internal threats	96	27
Online fraud	93	25
Theft of business-critical data	92	18
Takeover of devices	80	25
Distributed denial-of-service (DdoS) attacks	79	35

Source: authors.

Based on the responses, we created two new variables: the number of known types of threats and the number of types of threats experienced. For each respondent, we calculated the values by adding up the affirmative responses for each type of threat. On average, respondents were familiar with six out of nine types of threat ($M = 6.0$, $SD = 2.8$), while on average they reported experiencing two incidents ($M = 2.2$, $SD = 2.2$). Both variables are approximately normally distributed (skewness and kurtosis from −2 to 2).

Table 4. Average trust scores for different security solutions

Passwords for entering computer systems	3.9	0.9	−0.8	0.6
PIN code for unlocking a SIM card	3.8	1.1	−0.9	0.3
PIN for accessing smartphone applications	3.8	0.9	−1.0	1.5
Antivirus protection	3.8	1.0	−1.1	1.3
VPN connection	3.8	1.0	−0.7	0.3
Data encryption	3.7	1.0	−0.7	0.3
Authentication required for using certain functions	3.7	1.0	−0.9	0.8
Enabled device tracking in case of theft	3.7	1.0	−0.7	0.5
Remote device wipe	3.6	1.0	−1.4	−0.1
Archiving smartphone contents	3.6	0.9	−0.4	0.2
Archiving laptop and desktop contents	3.6	0.9	−0.5	0.2
Centralised control over a smartphone	3.5	1.0	−0.6	0.3

Note: *M* – mean; *SD* – standard deviation.
Source: authors.

Next, we measured trust in information security solutions by asking respondents to what extent they trust individual solutions when using ICT. They responded on a 5-point scale from 1 (*I do not trust it at all*) to 5 *(I fully trust it*), with 12 different security solutions listed. Table 4 shows the average values of the responses, their variability, and the coefficients of asymmetry and kurtosis, which indicate an approximately normal distribution of responses to all statements. The average values show that people trust passwords for accessing computer systems, PIN codes, antivirus protection, and VPN connections the most. On average, they trust centralized control over smartphones the least.

Although skewness and kurtosis values indicated approximately symmetric distributions for all the variables, Shapiro-Wilk tests of normality were statistically significant ($p < 0.001$), suggesting deviations from normality. However, given the small sample size ($n = 125$) and the fact that skewness and kurtosis values remained within acceptable ranges (approximately ±1), these deviations were considered minor. Parametric tests that were conducted are known to be robust to such violations of normality.

5. Results

5.1. Factor analysis

We analyzed the probability of reporting an information security incident separately for smartphones and computers using exploratory factor analysis. For each device, we identified one factor that combines the probability of reporting to all of the above-mentioned institutions, except for IT experts at the hotel. The probability of reporting was significantly higher for this variable than for other institutions, so it did not fit into the factor structure. We joined the remaining variables into factors: probability of reporting (computer) and probability of reporting (phone), which we confirmed with confirmatory factor analysis (CAF). This was performed using the principal axis factoring method without rotation. In both cases, Bartlett's test of sphericity ($p < 0.001$) and the Kaiser-Meyer-Olkin (KMO) measure (0.84 for computer and 0.83 for smartphone) confirmed the suitability of the data for factor analysis. High factor weights (all between 0.63 and 0.89) indicate a good fit of the data to the model. The reliability of both factors was assessed using Cronbach's alpha coefficient, which was 0.912 for the likelihood of reporting (computer) factor and 0.9 for the likelihood of reporting (smartphone) factor, indicating high internal consistency of both factors. The new variables are approximately normally distributed, averaging at 2.8 ($M = 2.8$, $SD = 1.1$ for computer and $M = 2.8$, $SD = 1.0$ for smartphone).

We also investigated trust in information security solutions using exploratory factor analysis, performed using the principal axis factoring method and direct oblimin rotation due to the high interdependence of factors. Bartlett's test of sphericity ($p < 0.001$) and the KMO measure (0.81) confirm the suitability of the data for factor analysis. We identified two factors with weights of variables between 0.44 and 0.90, namely trust (codes) (PIN code for unlocking SIM cards, PIN for accessing applications, passwords for logging into computer systems), and trust (other) (all other

security solutions listed above). Their reliability is good, with Cronbach's alpha coefficients of 0.828 for trust (codes) and 0.894 for trust (other), with distributions approximately normal and averages of around 3.8 and 3.7 ($M = 3.8$, $SD = 0.9$ for trust [codes] and $M = 3.7$, $SD = 0.7$ for trust [other]).

5.2. Multiple linear regression

Next, we performed multiple linear regression to examine the relationships between the previously identified factors, with the probability of incident reporting as the dependent variable and the independent variables: number of known threat types, number of threat types experienced, trust in security solutions (other), and trust in security solutions (codes). We did not include demographic variables in the model as controls, as we assume that demographic characteristics are not a primary source of bias or correlation with the dependent variables. Additionally, we took into account the small size of our sample, which could lead to overfitting and instability of the model if demographic variables were included.

We checked for possible multicollinearity by calculating Pearson's correlation coefficients between independent variables, which were much lower than 0.8 in both models. In addition, the variance inflation factors (VIF) were between 1.0 and 1.6 in all cases, which also indicates the absence of multicollinearity. The assumptions of homoscedasticity and normal distribution of errors around a zero mean were assessed using graphical diagnostics. Visual inspection of standardized residuals within histograms indicated that the residuals were approximately normally distributed. Furthermore, scatterplots of standardized residuals against predicted values did not reveal any systematic patterns suggesting homoscedasticity. The obtained regression models (see Figure 1), i.e. for the probability of reporting an incident on a computer and the probability of reporting an incident on a phone, are statistically significant ($p < 0.05$). We identified similar statistically significant correlations in both models. The results indicate that a greater number of known cyber threat types is associated with a lower likelihood of reporting cybersecurity incidents to external institutions, providing support for H_{2a}. Conversely, higher trust in cybersecurity solutions beyond basic authentication mechanisms is associated with a higher likelihood of external incident reporting, supporting H_{2b}. No statistically significant associations were observed between these variables and internal reporting to hotel IT experts, suggesting that internal reporting behaviour may be less sensitive to individual differences in knowledge and trust.

The findings show that individuals who are familiar with more different types of threats are less likely to report a security incident to an institution outside the organization. Conversely, greater trust in other information security solutions (not codes) is associated with a higher likelihood of reporting incidents that occur on both personal computers and smartphones. The remaining two independent variables – the number of types of threats experienced and trust in security solutions (codes) – did not show a statistically significant correlation with the dependent variables.

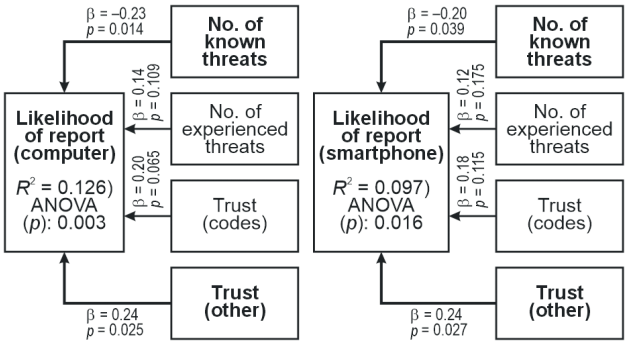

Figure 1. Regression models for 'Probability of reporting an incident' on computer (left) and smartphone (right)
Source: authors

Similarly, we checked the correlation between the same independent variables and the probability of reporting to an IT expert in the company, for which no statistically significant correlation was found at a significance level of $\alpha = 0.05$. Regardless of the number of known and experienced threats and confidence in security solutions (codes), respondents are equally likely to report a security incident to an IT professional. At a significance level of 0.1, however, there is a statistically significant negative correlation between trust in other security solutions and the likelihood of reporting to an IT expert. People who have more trust in other, more complex security solutions are less likely to report an incident to an IT expert in the company.

5.2.1. Independent samples *t*-test

To further explore differences in the likelihood of reporting incidents to institutions outside the organization based on specific types of threats, we tested for each type of threat whether the average assessment of the likelihood of reporting an incident differed between individuals who were aware of the threat and those who were not. For some types of threats, we found that the average probability of reporting an information security incident to external institutions is lower among those who are familiar with these threats, which is consistent with the findings of linear regression. This applies to the following types of threats, where the difference in averages was statistically significant, namely for computers: information system intrusion ($t = -4.24$, $p < 0.001$), theft of business-critical

data (t = −2.49, p = 0.014), malware infection (t = −2.90, p = 0.004), phishing (t = −2.63, p = 0.009) and online fraud (t = −2.25; p = 0.026), and for smartphones: information system intrusion (t = −3.12, p = 0.002), malware infection (t = −2.44, p = 0.016) and phishing (t = −2.47, p = 0.015). To ensure robustness, nonparametric tests (Mann-Whitney U tests) were additionally conducted to test the differences. The results were consistent with those obtained from parametric tests, supporting the validity of the conclusions.

6. Discussion

The findings of the study offer an in-depth insight into the behavioral, organizational and psychological patterns of employees in the hotel industry in the context of cybersecurity. Employees' strong trust in internal IT experts is reflected in a significantly higher likelihood of reporting incidents internally, suggesting that accessibility and perceived competence play a key role in reporting decisions. This finding supports H_1, indicating that employees are significantly more likely to report cybersecurity incidents to internal IT experts than to external institutions, which can be explained by higher perceived accessibility and trust. This suggests the importance of internal organisational structures, where personal contact, accessibility and recognition of an IT expert influence the likelihood of timely reporting, as it supports the view that effective threat management is not based solely on technical solutions, but on relationships and the structure of communication channels within the hotel. Similar trends are confirmed by Magliulo (2016), who finds that perceived closeness and trust in colleagues strongly influence operational decisions in crisis situations.

Importantly, external channels differ in their perceived implications. Low reporting likelihood to law enforcement may reflect expectations of formal procedures and uncertainty about outcomes, whereas low reporting to technical coordination bodies (e.g. CERT) may indicate limited awareness of their support role and unclear internal escalation protocols. Similarly, reluctance to contact the data protection authority may be linked to concerns about compliance scrutiny or lack of knowledge about notification obligations.

The low probability of reporting cybersecurity incidents to external institutions indicates a limited willingness among employees to engage with external authorities, which may reflect insufficient awareness of formal reporting procedures and uncertainty about institutional roles, as noted in prior research (Fragnière & Yagci, 2021). This may reflect gaps in employees' awareness of institutional roles and reporting procedures, which can limit effective cooperation with external cybersecurity stakeholders. An analysis of the correlation between knowledge of cyber threats and employee behavior offers an interesting insight. The findings support H_{2a}, indicating that employees' knowledge of cyber threats is associated with a lower willingness to report incidents to external institutions. At the same time, H_{2b} is supported, as higher trust in advanced cybersecurity solutions is associated with a greater likelihood of external reporting. Importantly, these associations are observed primarily for external reporting channels, whereas internal reporting to hotel IT experts appears to be relatively stable across different levels of knowledge and trust. More technically skilled employees may rely more on their own judgement, reducing their perceived need for external reporting. The OECD (2024) and Kruse et al. (2017) point out that a high level of self-confidence stemming from technical knowledge can create an illusion of control, reducing the perceived need for formal intervention. Conversely, less technically skilled employees are more likely to report incidents, especially to external institutions. This behaviour indicates a higher degree of caution or uncertainty, which may lead to faster detection of incidents, but may also reflect a perceived lack of organisational support within the hotel. This discrepancy raises the question of how to design training strategies that not only transfer knowledge but also build awareness of correct procedures, the ability to use one's own judgment and the importance of cooperation with external partners.

The survey also revealed clear preferences regarding trust in security solutions. Employees trust basic mechanisms, such as passwords, PIN codes, antivirus programs and VPN connections, more. These are tools they encounter on a daily basis and are easy to use. Users' trust in established technologies often does not extend to advanced security mechanisms such as multifactor authentication, encryption or tokenization, which individuals might perceive as overly complex, difficult to understand or unnecessary. Chen and Fiscus (2018) and Perwej et al. (2021) found that users often remain loyal to technologies they understand and are less likely to adopt new solutions, even if they are more effective in terms of security.

Higher trust in more complex security solutions is associated with a greater likelihood of external reporting and a lower likelihood of internal reporting. This may reflect differences in perceived competence and familiarity with advanced security mechanisms. Srivastava et al. (2022) confirm that the complexity of the threat influences the decision of whom an individual trusts in the resolution process. These findings are consistent with protection motivation theory, suggesting that both threat appraisal (knowledge of cyber threats) and coping appraisal (trust in cybersecurity

solutions) play a central role in shaping channel-specific reporting behaviour.

Statistical analysis did not reveal any significant correlations between the number of known threats or trust in basic mechanisms and willingness to report an incident to an IT professional, but it did reveal a weak but statistically significant correlation between trust in advanced solutions and a lower likelihood of internal reporting. This further confirms the need to improve the integration of advanced security practices into existing hotel organizational structures so that employees do not perceive the internal IT professional as less professional or overly focused on routine tasks.

The findings of our study highlight that cybersecurity in the hospitality industry must go beyond technical protection. Security policies must cover behavioral, psychological and organizational dimensions – not just what we use, but also how and why. It is crucial that cyber protection is positioned as a strategic function within a broader risk management system, where training, organizational culture, internal protocols and cooperation with external stakeholders play an important role. Without an inclusive, comprehensive and strategic approach that connects technology, people and processes, the hotel industry will not be able to meet the challenges of the modern digital environment.

7. Conclusion

This study contributes to the growing body of hospitality cybersecurity research by highlighting that cybersecurity in hotels extends beyond the technical domain and is closely linked to organisational and behavioural factors. Within the limits of a cross-sectional and exploratory research design, the findings suggest that employees' attitudes toward cyber threats are associated with their knowledge of cyber risks, their trust in cybersecurity solutions, and their understanding of incident response procedures, all of which are embedded in the broader security culture of hotels.

The findings indicate that hotel employees show a strong preference for internal reporting, particularly to internal IT experts, who are perceived as the primary and most accessible point of contact in the event of a cybersecurity incident. This pattern underscores the importance of internal organisational structures and trusted communication channels in supporting timely incident response. At the same time, it raises questions about whether reliance on internal reporting alone is sufficient in cases that require broader coordination with specialised external institutions, such as national CERTs, law enforcement agencies or regulatory authorities.

The relatively low willingness to report incidents to external institutions observed in this study suggests potential gaps in employees' awareness of institutional roles, reporting obligations and expected outcomes of external reporting. Particular attention should therefore be given to improving employees' understanding of external reporting obligations, including when and how to engage with external institutions, as well as the expected outcomes of such reporting. While these findings do not allow causal conclusions, they point to possible risks related to delayed escalation or limited engagement with external support mechanisms. In this context, targeted training and clearer communication of reporting procedures may represent an important area for organisational improvement.

The findings further indicate that greater knowledge of cyber threats is associated with a lower likelihood of reporting incidents to external institutions, whereas lower levels of technical knowledge are associated with higher reporting propensity. Rather than implying superior or inferior behaviour, this pattern may reflect differences in perceived self-efficacy and uncertainty among employees, which appear to shape reporting preferences. This paradox highlights the importance of training strategies that balance technical competence with clear guidance on when and how formal reporting is appropriate.

In terms of cybersecurity solutions, the findings suggest that employees tend to place higher trust in familiar and easily understandable mechanisms, such as passwords, PIN codes, antivirus software and VPN connections, while trust in more advanced security solutions – such as encryption or multi-factor authentication – is comparatively lower. Although this study does not assess actual effectiveness, this finding points to a potential mismatch between employees' perceptions and contemporary cybersecurity standards, which increasingly rely on advanced protection mechanisms. This suggests the need for targeted awareness initiatives that explain the functionality and benefits of advanced cybersecurity solutions, particularly those perceived as complex (e.g. multi-factor authentication or encryption).

Based on these findings, several practical implications can be cautiously derived. Hotels may benefit from implementing differentiated training programmes that explicitly distinguish between internal and external reporting procedures, including scenario-based training on when incidents should be escalated to external institutions such as CERTs or regulatory authorities. In addition, establishing clear, transparent and user-friendly incident reporting procedures – including step-by-step escalation protocols, clearly defined responsibilities, and accessible reporting interfaces (e.g. internal digital platforms or anonymous reporting channels) – may help reduce uncertainty and

encourage timely reporting across different employee groups. Regular security audits and cooperation with external experts may further support organisational learning and preparedness.

This study is subject to several limitations. The data were collected from a non-random convenience sample of hotel employees in Croatia, which may introduce self-selection bias and limits the generalisability of the findings to other national or institutional contexts. Furthermore, demographic variables (e.g. job position, length of experience) were not included as control variables in the regression models due to sample size constraints, restricting the examination of their potential influence on reporting behaviour. Third, the cross-sectional nature of the study limits the ability to draw conclusions about changes in cybersecurity reporting behaviour over time. Finally, as the data are based on self-reported measures, responses may be subject to social desirability bias. Future research should address these limitations by employing larger, multi-country samples and longitudinal designs to explore changes in cybersecurity behaviour over time.

At a strategic level, the findings suggest that hotel management may consider integrating cybersecurity more explicitly into broader risk management and business planning processes, including the formalisation of incident response roles, regular simulation exercises and alignment with regulatory requirements such as reporting obligations under *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. As hotels increasingly resemble data-intensive service infrastructures, stronger alignment with regulatory frameworks – such as those introduced under the NIS2 Directive – may further enable more systematic, coordinated and resilient approaches to cybersecurity across the tourism sector.

Overall, this study reinforces the view that effective cybersecurity in hospitality cannot rely solely on technological solutions. Instead, it requires an integrated approach that combines technology, organisational processes, employee behaviour and institutional cooperation. Strengthening these interrelated elements may help hotels enhance their resilience to cyber threats while safeguarding both operational continuity and guest trust.

References

Alonso-Almeida, M. del M., & Giglio, C. (2024). Cybersecurity in tourism and hospitality management research: Current issues, trends, and an agenda for future research. *Cuadernos de Turismo*, (53), 243–260. https://doi.org/10.6018/turismo.616471

Arcuri, M.C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on the hospitality sector: Stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2), 277–290. https://doi.org/10.1108/JHTT-05-2019-0080

Bishop, L.M., Asquith, P.M., & Morgan, P.L. (2025). The employee cybersecurity awareness framework. *Human Behavior and Emerging Technologies*, Article 1025045. https://doi.org/10.1155/hbe2/1025045

Casais, B., & Ferreira, L. (2023). Smart and sustainable hotels: Tourism Agenda 2030 perspective article. *Tourism Review*, *78*(2), 344–351. https://doi.org/10.1108/TR-12-2022-0619

Chang, S.E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*(3), 438–458. https://doi.org/10.1108/02635570710734316

Chen, H.S., & Fiscus, J. (2018). The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. *Journal of Hospitality and Tourism Technology*, *9*(2), 223–234. https://doi.org/10.1108/JHTT-07-2017-0044

Chen, H.S., & Jai, T.-M.(C.). (2019). Cyber alarm: Determining the impacts of hotel's data breach messages. *International Journal of Hospitality Management*, *82*, 326–334. https://doi.org/10.1016/j.ijhm.2018.10.002

de Bruin, M., & Mersinas, K. (2024). *Individual and contextual variables of cyber security behaviour: An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour*. [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2405.16215

European Parliament and Council of the European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555

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. https://doi.org/10.3390/smartcities7010019

Florido-Benítez, L. (2025). The role of cybersecurity as a preventive measure in digital tourism and travel: A systematic literature review. *Discover Computing*, *28*, Article 28. https://doi.org/10.1007/s10791-025-09523-3

Fragnière, E., & Yagci, K. (2021). Network & cybersecurity in hospitality and tourism. In C. Cobanoglu, S. Dogan, K. Berezina & G. Collins (Eds.), *Hospitality & tourism information technology* (pp. 1–21). USF M3 Publishing. https://digitalcommons.usf.edu/m3publishing/vol17/iss9781732127593/7/

Johnston, A.C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. https://doi.org/10.2307/25750691

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*(7), 509–520. https://doi.org/10.1016/j.cose.2009.04.006

Kruse, C.S., Frederick, B., Jacobson, T., & Monticone, D.K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263

Maddux, J.E., & Rogers, R.W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Magliulo, A. (2016). Cyber security and tourism competitiveness. *European Journal of Tourism, Hospitality and Recreation*, *6*(2), 128–134. https://doi.org/10.1515/ejthr-2016-0015

National CERT (CERT.hr). (2025, March 25). Godišnji izvještaj rada Nacionalnog CERT-a za 2024. godinu [*Annual report on the work of the National CERT for 2024*]. https://www.cert.hr/godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2024-godinu/

Organisation for Economic Co-operation and Development. (2017). *Enhancing the role of insurance in cyber risk management*. OECD Publishing. https://doi.org/10.1787/9789264282148-en

Organisation for Economic Co-operation and Development. (2024, June). *New perspectives on measuring cybersecurity* (OECD Digital Economy Papers No. 366). OECD Publishing. https://doi.org/10.1787/b1e31997-en

Ozturk, A.B. (2026). Applying protection motivation theory to hotel employees' compliance with information systems security policies: The moderating role of generational differences. *Journal of Hospitality and Tourism Technology*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JHTT-01-2025-0035

Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N., & Jaiswal, A.K. (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Pipyros, K., & Liasidou, S. (2025). A new cybersecurity risk assessment framework for the hospitality industry: Techniques and methods for enhanced data protection and threat mitigation. *Worldwide Hospitality and Tourism Themes*, *17*(1), 48–61. https://doi.org/10.1108/WHATT-12-2024-0296

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Srivastava, G., Jhaveri, R.H., Bhattacharya, S., Pandya, S., Rajeswari, R., Maddikunta, P.K.R., Yenduri, G., Hall, J.G., Alazab, M., & Gadekallu, T.R. (2022). XAI for cybersecurity: State of the art, challenges, open issues and future directions. *ACM Computing Surveys*, *1*(1). https://doi.org/10.48550/arXiv.2206.03585

Yallop, A.C., Gică, O.A., Moisescu, O.I., Coroș, M.M., & Séraphin, H. (2023). The digital traveller: Implications for data ethics and data governance. *Journal of Consumer Marketing*, *40*(2), 155–170. https://doi.org/10.1108/JCM-12-2020-4278