THE IMPACT OF EMPLOYEE CYBERSECURITY AWARENESS ON THE OVERALL SECURITY OF SMALL HOTELS

Anastasiia Mokhonko, Artjoms Musaeļans, Gabriel Wang, Niels Meijer and Petar Paskalev

1 INTRODUCTION

Within an era characterized by technological advancement and the extensive influence of digital transformation, Small and Medium Enterprise (SME) assumes a pivotal role in the economic landscape (Arroyabe et al., 2024), as well as facing growing threats from cyberattacks. A survey at National Center for the Middle Market (2016) highlights that "55% of SME companies lack either an up-to-date cyber-risk strategy or any defined cyber-risk strategy at all" (Benz and Chatterjee, 2020). For instance, SMEs in the tourism sector, particularly small hotels, often operate with limited resources and expertise, making them especially vulnerable to data breaches, phishing, and other cybersecurity threats. In today's digital landscape, cybersecurity preparedness is crucial for their survival and long-term success, and cannot be overlooked.

One key factor in mitigating these threats in question is employees' cybersecurity awareness, which encompasses the knowledge, behaviors, and attitudes that staff members possess regarding cybersecurity threats. This awareness includes understanding common attack methods such as phishing, malware, and social engineering, as well as recognizing the importance of strong password management, secure handling of data, and adherence to company protocols. Employees who are well-trained in these areas can identify potential threats more effectively and respond appropriately, reducing the likelihood of breaches or compromises. Furthermore, consistent application of these best practices by all team members strengthens the organization's overall security status, minimizing vulnerabilities and ensuring that sensitive information and critical systems are safeguarded from malicious activities.

After conducting a study of the relevant literature mentioned in the below section, it became evident that while much of the current research emphasizes the significance of employee training in enhancing cybersecurity awareness, it primarily focuses on broad recommendations for SMEs. However, there is a significant gap regarding specific training methods and best practices suited to small hotels, which operate with unique constraints, such as limited budgets and resources. This study aims to contribute to the existing body of research by addressing this overlooked area and offering practical insights into how to tailor cybersecurity training to the specific needs of small hotels.

Building upon this gap, our research will investigate key factors influencing employee cybersecurity awareness in small hotels, such as personal attitudes, the presence of an in-house IT specialist, and the frequency of training. By focusing specifically on these under-researched aspects within SMEs, this study seeks to provide a deeper understanding of effective cybersecurity practices in a sector that has been largely neglected in existing studies.

To achieve this, we will conduct a comprehensive literature review, supplemented by surveys and interviews with employees from small hotels. The data will be analyzed using appropriate statistical methods to address our specific research questions. Ultimately, the findings will offer actionable recommendations designed to improve cybersecurity awareness and practices in SMEs, thus filling a critical gap in current research.

1.1 Research Question

1.1.1 The relevance

Cybersecurity Awareness in the Hospitality Industry: Small hotels handle a lot of sensitive customer information and rely heavily on digital systems, making them prime targets for cyberattacks. However, they often don't have the resources to build strong cybersecurity defenses. This research focuses on how boosting employee awareness around cybersecurity can strengthen overall security and help protect against data breaches.

1.1.2 The story

These subquestions are key because they explore how employee views and the presence of an IT specialist can impact cybersecurity practices in small hotels. Regular training might improve adherence to security protocols, and effective

training could reduce the costs of data breaches. Understanding how hotels educate their staff on cybersecurity is crucial for finding the best ways to boost security in resource-limited settings. Together, these questions reveal the role of employee awareness in protecting small hotels from cyber threats.

*How does employee cybersecurity awareness impact **the overall** security of small hotels?*

To provide an answer to this research question, we have come up with the following sub-questions:

1. Do the personal opinions of employees affect their approach to cybersecurity concerns?
2. Does the presence of an in-house IT specialist improve the cyber security awareness of hotel employees?
3. Does the frequency of cybersecurity training affect employee adherence to cybersecurity practices in small hotels?
4. Do the employees' ages correlate with their level of cybersecurity awareness?
5. How do small hotels educate their employees on cybersecurity practices?

2 LITERATURE STUDY

2.1 The Impact of Employee Cybersecurity Awareness on the Security Posture of Small Hotels

The cybersecurity landscape in the hospitality industry is increasingly shaped by complex threats, especially due to the vast amounts of sensitive customer data collected by businesses like hotels. Small hotels, in particular, are vulnerable to cyber-attacks because they often lack the financial and technological resources necessary to implement robust defences. This issue is further compounded by a general lack of employee cybersecurity awareness, which contributes significantly to the industry's susceptibility to breaches. Several studies emphasize that improving employee cybersecurity awareness can greatly enhance an organization's security posture. Research indicates that breaches frequently result from human error, such as falling victim to phishing attacks or failing to secure Wi-Fi networks. Thus, employee training becomes crucial to minimize vulnerabilities and build resilience against cyber threats in the hospitality sector (Afolabi (2024), Shabani and Munir (2020), Negussie (2023))

Our research will build on these insights by examining how cybersecurity training specifically impacts small hotels' incident response and long-term security culture. This approach will not only focus on preventing breaches but also aim to provide a framework for recovery and resilience, tailored to the limited resources of small hotels.

2.2 Cybersecurity Challenges in Hospitality and the Role of Employee Awareness

One prominent study by **UpGuard (2024)** outlines the specific cybersecurity vulnerabilities faced by the hospitality industry, including point-of-sale (POS) systems, unsecured hotel Wi-Fi, and Internet of Things (IoT) devices. The research highlights that small hotels are frequent targets for cybercriminals because they collect vast amounts of personal and financial data. The study finds that employees' lack of awareness regarding phishing and social engineering attacks makes them prime entry points for cyber incidents, which can result in significant financial and reputational damage.

Verizon's Data Breach Investigations Report, Negussie (2023), human error was found to be a major factor in data breaches, particularly in sectors like hospitality, where cybersecurity awareness is often lacking. According to the report, many incidents, such as phishing and malware attacks, could have been prevented if employees were better trained to recognize and avoid suspicious activities. The findings underscore the importance of employee training in minimizing vulnerabilities caused by human error.

2.3 The Effectiveness of Cybersecurity Awareness Training

A comprehensive study by the **Aberdeen Group, Negussie (2023)** demonstrated the effectiveness of regular cybersecurity awareness training in reducing security incidents. The study involved multiple industries, including hospitality, and found that companies implementing ongoing training programs experienced a 70% reduction in security breaches. This study is significant for small hotels because it indicates that even with limited technical defences, investing in human capital through training can greatly enhance security. Hotels that provide their employees with the knowledge to identify phishing emails, malicious links, and insecure networks are better positioned to prevent incidents from escalating.

Another study conducted by **Coventry et al. Truță (2024)** focused specifically on cybersecurity training in small businesses. The research found that employee training leads to measurable improvements in adherence to security protocols and incident reporting. For small hotels, this means that a relatively low-cost investment in training can help reduce the risk of successful cyberattacks, which often target employees through social engineering tactics. The study also emphasizes the need for tailored training programs, particularly for employees with less technical expertise, to maximize the effectiveness of these interventions.

2.4 Building a Cybersecurity-Conscious Culture

A study by **the SANS Institute, Spitzner (2021)** explored the long-term effects of cybersecurity training on organizational culture. The research concluded that regular, consistent training fosters a cybersecurity-conscious culture, where employees are not only aware of risks but actively engaged in maintaining secure practices. This cultural shift was shown to significantly reduce the likelihood of breaches caused by negligence or oversight. In the context of small hotels, this finding is critical, as a strong cybersecurity culture can offset some of the resource limitations that prevent smaller organizations from investing in more sophisticated technical solutions.

This is echoed in a **Rhee et al., Afolabi (2024)** , which found that companies with a strong cybersecurity culture were better able to detect and mitigate risks early, often before they caused substantial harm. The study suggests that when employees are regularly trained and involved in security processes, they become more vigilant, which enhances the organization's overall resilience. For small hotels, building such a culture can be a cost-effective way to bolster cybersecurity without the need for extensive technology investments.

2.5 Employee Training and Incident Response

A study conducted by **the Ponemon Institute Community (2020)** focused on the role of employee training in effective incident response. The study surveyed over 500 organizations across various industries, including hospitality, and found that businesses with well-trained employees had faster response times to cybersecurity incidents. These organizations were able to contain breaches more quickly, reducing the overall damage and recovery costs. For small hotels, where downtime due to a cyberattack can be particularly devastating, having employees who know how to respond to breaches can make a substantial difference in recovery outcomes.

Additionally, a study by **IBM Security, IBM (2021)** reported that companies with trained employees were able to reduce the cost of a data breach by an average of 50%. This underscores the importance of not only providing initial training but also continually reinforcing cybersecurity practices through regular drills and updates. Small hotels that incorporate these practices can mitigate the financial risks associated with cyberattacks, even if their technological defences are relatively modest.

2.6 Technological Solutions Enhanced by Employee Awareness

While employee awareness is a critical component of a strong cybersecurity posture, several studies have shown that combining training with basic technological measures is most effective. A study by Shabani and Munir (2020) on cybersecurity in the hospitality sector found that organizations using encryption, secure Wi-Fi, and multi-factor authentication (MFA) experienced fewer breaches. However, the study also found that these measures were only fully effective when employees were trained to use them properly. For example, encrypted data can still be compromised if employees unknowingly share passwords or connect to insecure networks.

A similar study by **Ekran System (2024)** concluded that cybersecurity tools, such as firewalls and endpoint detection systems, are most successful when integrated with employee training programs. Employees must understand how these tools work and the critical role they play in overall security. For small hotels, where budget constraints may limit the adoption of advanced technologies, the combination of training and basic security tools offers a feasible path to improved cybersecurity.

2.7 Conclusion

The literature reviewed highlights that employee cybersecurity awareness is a key component in improving the overall security posture of small hotels. Studies consistently demonstrate that training employees to recognize and respond to threats reduces the likelihood of successful cyber incidents, especially in sectors like hospitality, where human error is frequently exploited. Research from UpGuard (2024) and Negussie (2023) emphasizes the specific risks tied to employee behaviour, such as falling victim to phishing or failing to secure networks. Furthermore, research from Shabani and Munir (2020) indicates that even basic technological solutions like encryption and multi-factor authentication are only fully effective when paired with proper employee education.

While previous research has established the foundational importance of training, our research aims to extend these findings by focusing on how employee awareness impacts small hotels' ability to respond to and recover from cyber incidents. The addition lies in investigating not only general security posture improvements but also the tangible effects on incident response times, recovery costs, and long-term security culture development. This approach can provide small hotels with a more actionable framework for integrating employee training into their broader cybersecurity strategies.

3 METHODOLOGY

In this research article, we will conduct quantitative and qualitative research methods to answer the research question proposed in this paper. For this reason, we will be conducting a survey as well as several interviews with industry professionals and testing their knowledge of cybersecurity. We do this to connect both actual knowledge and their estimated knowledge with the actual risk of working in a small or medium enterprise (SME). Our participants are selected by our shared network and SMEs working together with DigiWerkplaats. This research will be conducted with a convenience sampling method. During our study, we will meet with a variaty of business owners within the hospitality business as well as their employees.

When creating the survey, we will ask closed questions to gauge their knowledge of cybersecurity and how they estimate their knowledge. This will be compared to actual risks faced in hospitality.

For this paper, we will use several statistical methods to analyze our survey data. Interviews will be recorded using iPhone 11 and transcribed. The interviews will be analyzed using thematic and content analysis. To conduct this analysis we will use Python, scikit-learn and jupyter notebook to process our data. The surveys are made using Qualtrics. For reliability,

questions will be repeated in different phrasings and, compare the answers to ensure consistency.
Due to the sampling method and small sample group, this study is only meant as a guideline or pilot study. Each participant will be provided with an informed consent letter. A data management plan will also be put into place that is compliant with the GDPR. Participants will remain anonymous. Data can only be viewed by researchers working on this paper.

4 Stakeholder Analysis: SMEs in the Hospitality Business

4.1 Stakeholder Needs and Concerns:

Limited Resources: Small and medium-sized enterprises (SMEs) in the hospitality industry usually operate on tight budgets, lacking financial resources and dedicated cybersecurity expertise. They require cost-effective, practical cybersecurity solutions that are easy to implement.

Cybersecurity Threats: These businesses face increasing threats, such as data breaches, ransomware, and phishing attacks, which can harm their reputation and lead to financial loss.

Employee Awareness: Many SMEs have non-technical staff who might not be well-trained in recognizing and preventing cyber threats. Improving cybersecurity awareness is essential to mitigate risks caused by human error.

Customer Trust: As hospitality businesses collect and store a significant amount of sensitive customer information (e.g., payment details, and personal identification), protecting this data is critical to maintaining customer trust and loyalty.

Compliance: SMEs in hospitality need to adhere to regulations like GDPR, requiring them to manage and protect customer data responsibly.

4.2 How These Needs Shaped the Research Question:

Focus on Cybersecurity Awareness: Since many SMEs lack the resources to invest in advanced technical solutions, the research question emphasizes employee cybersecurity awareness. This reflects the practical needs of SMEs, where human behaviour and internal practices play a critical role in security due to the lack of advanced tools. Research Question: ”How does employee cybersecurity awareness impact the overall security of small hotels?” This directly addresses the concern that, in many SMEs, human error is a primary vulnerability.

Relevance to Hospitality SMEs: The choice to focus specifically on small hotels stems from recognizing that these businesses handle sensitive customer information (reservations, payment details) and are vulnerable to cyberattacks. The research question is tailored to explore how improving employee awareness can enhance overall security in this context.

Training and Awareness Programs: SMEs in hospitality often lack the budget to hire dedicated IT specialists. The research explores whether enhancing employee awareness through cost-effective training programs can compensate for this gap, providing actionable insights into how hotels can improve their security posture without major financial investments.

Exploring the Human Element: Instead of focusing purely on technical defences, the research highlights the human element of cybersecurity. This reflects the stakeholder reality that SMEs may already have basic tools (e.g., firewalls) but suffer from a lack of staff understanding and adherence to security protocols.

4.3 Conclusion:

The stakeholder analysis of SMEs in the hospitality industry shaped the research question by emphasizing practical, human-centred approaches to cybersecurity. Given the resource constraints and the reliance on non-technical staff in these businesses, the focus on employee awareness and cost-effective training programs aligns with the stakeholders' most pressing needs. The research is designed to provide actionable insights that can help SMEs strengthen their security posture without requiring extensive investments in technology or specialized personnel.

5 Predicted Outcomes

Our research is focused on understanding the impact of employee cybersecurity awareness on the overall security condition of small hotels. Each sub-question delves into a specific factor that contributes to this broader issue. By investigating these factors, we expect to derive actionable insights that can help small hotel owners make informed decisions regarding cybersecurity policies and practices.

Do the personal opinions of employees affect their approach to cybersecurity concerns?

H_0**:** Personal opinions of employees do not significantly affect their approach to cybersecurity concerns.
H_1**:** Personal opinions of employees significantly affect their approach to cybersecurity concerns.
Variables:

- **Independent variable:** Personal opinions of employees (measured through a survey capturing attitudes towards cybersecurity).
- **Dependent variable:** Employee cybersecurity behavior (measured through adherence to security policies, frequency of reported incidents, and compliance with protocols).

Predicted Outcome: We anticipate that employees who personally prioritize cybersecurity and regard it as a crucial component of their responsibilities will demonstrate elevated levels of adherence to cybersecurity protocols. Individual perspectives on the significance of cybersecurity may result in more prudent conduct, including enhanced password protocols, improved compliance with security regulations, and an increased readiness to report anomalous actions. In contrast, employees who regard cybersecurity as a minor concern or believe it is only the IT department's job may demonstrate less vigilant behavior, hence heightening the danger of breaches. This result will highlight the significance of cultivating a cybersecurity-aware culture in which employees are driven to act responsibly, not alone owing to company standards but also from a personal dedication to security.

We also expect that this relationship may differ based on the employees' positions inside the hotel. Frontline personnel, who may infrequently engage with sensitive client data, can exhibit diminished motivation to adhere to rigorous security protocols in contrast to administrative staff responsible for managing booking and payment information. Comprehending these distinctions will aid in formulating specialized training programs that can connect personal perspectives with the company's cybersecurity aims.

Does the presence of an in-house IT specialist improve the cybersecurity awareness of hotel employees?

H_0**:** The presence of an in-house IT specialist does not significantly improve the cybersecurity awareness of hotel employees.
H_1**:** The presence of an in-house IT specialist significantly improves the cybersecurity awareness of hotel employees.
Variables:

- **Independent variable:** Presence or absence of an in-house IT specialist.
- **Dependent variable:** Cybersecurity awareness of hotel employees (measured through knowledge assessments, employee feedback, and self-reported familiarity with security protocols).

Predicted Outcome: We expect that the inclusion of an in-house IT specialist will substantially enhance employees' cybersecurity understanding. An IT specialist offers continuous instruction and may resolve security issues in real-time. They possess the capability to tailor cybersecurity training to address the hotel's particular requirements and vulnerabilities.

Moreover, employees are more inclined to regard cybersecurity with seriousness when an internal expert elucidates the ramifications of breaches in comprehensible language. Hotels lacking an in-house IT professional may depend on third-party services that may not be as accessible or as knowledgeable about the hotel's specific operations. Consequently, we anticipate that hotels employing an in-house specialist will exhibit fewer security breaches, and that their staff will display greater adherence to security protocols.

This outcome highlights the importance of investing in dedicated cybersecurity personnel, particularly for hotels that handle significant volumes of customer data and online transactions.

Does the frequency of cybersecurity training affect employee adherence to cybersecurity practices in small hotels?

H_0**:** The frequency of cybersecurity training does not significantly affect employee adherence to cybersecurity practices.
H_1**:** The frequency of cybersecurity training significantly affects employee adherence to cybersecurity practices.
Variables:

- **Independent variable:** Frequency of cybersecurity training (measured by the number of training sessions per year).
- **Dependent variable:** Employee adherence to cybersecurity practices (measured through compliance rates with security protocols, frequency of reported security incidents, and post-training surveys).

Predicted Outcome: We expect that increased frequency of training sessions correlates with improved compliance with cybersecurity protocols among personnel. Regular training maintains cybersecurity awareness among staff, ensuring they remain informed about emerging risks and optimal procedures. Consistent reinforcement of essential principles reduces the likelihood of employees forgetting critical security practices or becoming complacent.

Furthermore, consistent training can facilitate the identification and rectification of deficiencies in employees' expertise. We expect that hotels providing annual or biannual training will achieve greater compliance with security standards than those that give training solely during employee onboarding or intermittently. Training incorporating real-world scenarios, interactive components, and current information on emerging hazards is likely to be the most effective in fostering employee engagement and knowledge retention.

This anticipated result indicates that hotels ought to regard cybersecurity training as a continuous endeavor rather than a singular occurrence, emphasizing that regular, interactive training is crucial for mitigating human error, a primary contributor to security breaches.

Do the employees' ages correlate with their level of cybersecurity awareness?

H_0**:** Employee age does not significantly correlate with their level of cybersecurity awareness.
H_1**:** Employee age significantly correlates with their cybersecurity awareness level.

Variables:

- **Independent variable:** Employee age (measured by age group categories).
- **Dependent variable:** Level of cybersecurity awareness (measured by knowledge assessments, self-reported awareness, and adherence to security protocols).

Predicted Outcome: We predict that employee age will have a notable association with cybersecurity awareness. Younger employees, who are often more exposed to technology in their everyday lives, may demonstrate higher baseline awareness of cybersecurity issues, as they are more likely to encounter discussions about online threats in both personal and professional contexts. On the other hand, older employees might exhibit lower levels of cybersecurity awareness due to less frequent engagement with digital security issues, especially if they did not grow up in a digital-first environment.

However, we also anticipate variability within each age group, as exposure to cybersecurity training, personal interest, and specific job roles may play a significant role in shaping awareness. This outcome will suggest that age-targeted training programs could help close any gaps in cybersecurity knowledge across different age groups, ensuring that all employees, regardless of age, are equally prepared to handle cybersecurity threats.

How do small hotels educate their employees on cybersecurity practices? (Qualitative)

This sub-question requires a qualitative exploration of how small hotels educate their employees about cybersecurity. The research will focus on identifying patterns and themes in training methods, using interviews, focus groups, and content analysis.

H_0**:** There is no significant variation in how small hotels educate their employees on cybersecurity practices.
H_1**:** There is significant variation in how small hotels educate their employees on cybersecurity practices.

Variables:

- **Independent variable:** Methods of employee education (e.g., formal training, informal briefings, or self-learning).
- **Dependent variable:** Employee understanding and adherence to cybersecurity practices (qualitatively assessed via interviews or focus groups).

Predicted Outcome: We anticipate that hotels investing in extensive, dynamic, and ongoing educational programs will experience elevated cybersecurity awareness and improved compliance with security protocols among their staff. Hotels employing sporadic or unstructured techniques may have staff that are less cognizant of specific dangers and the requisite protocols to minimize those risks.

Furthermore, hotels that utilize many educational approaches, such as online training modules, in-person workshops, and regular updates via email or staff meetings, are likely to get superior outcomes compared to those that depend on a singular educational approach. A diverse methodology enables employees to interact with the content through many modalities, enhancing retention and comprehension.

We estimate that individuals subjected to regular knowledge assessments and mandatory participation in security drills will be more equipped to manage real-world dangers than those who receive solely theoretical instruction. This discovery will underscore the necessity for pragmatic, scenario-driven education to ensure that personnel are not merely passively receiving information, but are actively acquiring skills to address future security issues.

REFERENCES

Afolabi, G. J. (2024). Cybersecurity challenges and solutions for small businesses. *Research Gate*.

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., and de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, 141:103826.

Benz, M. and Chatterjee, D. (2020). Calculated risk? a cybersecurity evaluation tool for smes. *Business Horizons*, 63(4):531–540.

Community, I. S. (2020). Ponemon institute cost of a data breach report 2020: Key findings and best practices. https://community.ibm.com/community/user/security/events/event-description?CalendarEventKey=138799f1-67eb-475f-9832-a630417397c7. Accessed: 2024.

IBM (2021). Ibm report: Cost of a data breach hits record high during pandemic. Accessed: 20-09-2024.

Negussie, D. (2023). Importance of cybersecurity awareness training for employees in business. *Research Gate*.

Shabani, N. and Munir, A. (2020). A review of cyber security issues in hospitality industry. In Arai, K., Kapoor, S., and Bhatia, R., editors, *Intelligent Computing*, volume 1230 of *Advances in Intelligent Systems and Computing*, pages 462–474. Springer, Cham.

Spitzner, L. (2021). Why a strong security culture? Accessed: 20-09-2024.

System, E. (2024). Cybersecurity in hotels: Best practices & solutions. Accessed: 20-09-2024.

Truță, F. (2024). Why cybersecurity training and awareness are essential for any small business. Accessed: 20-09-2024.

UpGuard (2024). Cybersecurity in the hospitality industry: Protecting customer data. https://www.upguard.com/blog/cybersecurity-in-the-hospitality-industry. Accessed: 2024.