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

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

October 28, 2024

1 Executive Summary

This policy paper explores the importance of cybersecurity awareness in small hotels, with an emphasis on improving training practices to foster adherence to cybersecurity protocols. Given the increasing reliance on digital systems and the sensitive nature of customer data handled by small hotels, cybersecurity is paramount. However, small and medium enterprises (SMEs), including hotels, often face significant resource constraints, limiting their capacity to develop robust cybersecurity infrastructures (Afolabi, 2024; Chin, n.d.).

Our research examined the influence of cybersecurity training frequency, interactivity, and role-specific relevance on employee compliance with cybersecurity protocols. Essential findings demonstrate that consistent, interactive training sessions customized for certain positions can markedly improve cybersecurity compliance. Moreover, demographic variables, including age and gender, showed minimal impact on cybersecurity awareness, indicating that a standardized training method may be efficacious (Negussie, 2023). This paper offers pragmatic ideas to assist SME managers in the hospitality sector in executing efficient, economical cybersecurity policies that correspond with their operational requirements and resource constraints.

Keywords: cybersecurity, small hotels, training effectiveness, employee awareness, hospitality industry.

2 Stakeholder Analysis: SMEs in the Hospitality Business

The primary stakeholders of this research are small and medium-sized enterprises (SMEs) in the hospitality sector, with a specific focus on small hotels, as well as Digiwerkplaats, an organization that helps SMEs with the digital transformation of their companies. These businesses face significant challenges in managing cybersecurity due to limited financial and technical resources. Operating on tight budgets, small hotels often struggle to invest in advanced security tools or hire dedicated IT professionals. As a result, their major concerns and challenges in this matter are the exposure to cyber threats, including ransomware, phishing, and data breaches. Such incidents not only lead to financial losses but can also severely damage customer trust, a critical factor for success in the hospitality industry.

In addition to these financial constraints, employee cybersecurity awareness is a pressing concern. The workforce in small hotels often lacks formal training in identifying and mitigating cyber risks, making human error one of the primary vulnerabilities. Despite the presence of basic technical defenses like firewalls, the absence of employee understanding and adherence to security protocols frequently undermines these measures. Considering these issues, small hotels must comply with regulations such as the General Data Protection Regulation (GDPR), which requires strict management and protection of customer data. For many SMEs, complying with these regulatory requirements adds another layer of complexity to their operations.

Digiwerkplaats, the secondary but vital stakeholder, plays a critical role in supporting SMEs as they navigate these challenges. As an organization dedicated to enabling digital transformation for small businesses, Digiwerkplaats provides resources and expertise to help SMEs enhance their digital capabilities, including cybersecurity. Their mission originally formulated the goals of this research, particularly in addressing the lack of cybersecurity literacy among employees. Their primary need is to deliver cost-effective, scalable training programs that can be readily adopted by non-technical staff in small hotels. As a result, this research aims to provide actionable insights actionable insights into addressing the cybersecurity challenges faced by SMEs, particularly through employee training and awareness programs to meet their expectations.

Building on these identified concerns and expectations, we brought out the research question, “How does employee cybersecurity awareness impact the overall security of small hotels?” By focusing on the human element of cybersecurity, this study acknowledges the practical realities faced by SMEs. While technical defenses are important, the frequent gaps in employee awareness and behavior underscore the need for a human-centered approach to improving security. In alignment with Digiwerkplaats’s strategic objectives, we set our research focus on cost-effective solutions that emphasize training and education rather than expensive technological investments.

To ensure alignment with stakeholder needs, the research involves direct communications with SMEs and Digiwerkplaats by methods such as Microsoft Teams via BUas introduction and emails. Surveys and interviews with small hotel managers provided insights into their specific cybersecurity challenges and resource limitations. Collaboration with Digiwerkplaats facilitated the development of tailored training programs, emphasizing accessibility and relevance for non-technical employees. Regular consultations with both stakeholder groups ensured that the research outcomes would not only address immediate concerns but also offer sustainable, actionable solutions for enhancing cybersecurity resilience.

3 Introduction

Cybersecurity breaches are a growing threat to businesses across industries, with SMEs being particularly vulnerable due to limited financial and technical resources. For small hotels, the risk is compounded by the vast amounts of sensitive customer data they collect and store, including payment details and personal information (UpGuard, 2024). Despite these risks, cybersecurity practices are often underdeveloped in small hotels, leading to vulnerabilities that can be exploited by cybercriminals. Studies have shown that improving cybersecurity awareness can greatly enhance an organization's security posture (Kahraman et al., 2021; Negussie, 2023).

This policy paper addresses the need for enhanced cybersecurity training and awareness among employees in small hotels. By focusing on how training frequency, content relevance, and interactivity impact adherence to cybersecurity protocols, we aim to provide insights into how small hotels can strengthen their security posture. Unlike a technical research paper, this policy paper is intended for a non-technical audience, specifically SME managers, to help them understand the practical steps they can take to improve cybersecurity within their organizations.

The research conducted for this paper examines several key questions:

- How does the frequency of cybersecurity training affect employees' adherence to security practices?
- What are the current methods used by small hotels to educate employees on cybersecurity?
- Does the age of employees correlate with cybersecurity awareness levels?
- How do personal attitudes toward cybersecurity influence employees' adherence to security protocols?

By exploring these questions, this paper provides evidence-based recommendations for small hotels to develop more effective cybersecurity training programs that address the unique challenges of the hospitality industry.

4 Approaches and Results of Research

The research employed a mixed-methods approach, combining a quantitative survey and qualitative interviews to gather comprehensive insights. The data collected helped us identify patterns in how training frequency, employee roles, awareness, and adherence to protocols. Below, we present the key findings of this study.

1. Training Frequency and Adherence:
   Our research revealed a moderate positive correlation (r = 0.456) between the frequency of cybersecurity training and employee adherence to security protocols. Employees who received training at least quarterly were more likely to follow security guidelines in their daily tasks. However, increasing training frequency beyond a certain point (e.g., monthly) did not lead to proportional increases in adherence, suggesting that there is an optimal training frequency. Quarterly or biannual training sessions appear to balance engagement and effectiveness, avoiding the risk of "training fatigue," where employees may become disengaged if training is too frequent (Afolabi, 2024).

2. Role-Specific Needs and Relevance:
   The research found that employees with IT-related roles or greater experience in the field demonstrated higher levels of adherence to cybersecurity practices (Kahraman et al., 2021). This indicates that familiarity with cybersecurity concepts enhances training outcomes. Additionally, role-specific training tailored to the particular tasks and challenges faced by different departments (e.g., front desk, night shift) was found to be more effective than a generalized approach. Employees who perceived the training content as relevant to their specific roles applied cybersecurity practices more consistently in their daily routines.

3. Importance of Interactive Training Methods:
   Interactive training methods, such as scenario-based exercises and simulations, were found to significantly increase employee engagement and practical application of cybersecurity practices (UpGuard, 2024). Employees who participated in hands-on training retained information better and felt more prepared to handle real-world cyber threats. The qualitative data underscored that employees valued practical exercises over passive learning formats like online videos or presentations, which were associated with lower knowledge retention.

4. Uniform Knowledge Across Demographic Groups:
   Contrary to common perceptions, our analysis showed no significant difference in cybersecurity awareness levels across age groups. Both younger and older employees exhibited similar levels of knowledge and adherence, indicating that demographic factors like age do not necessarily influence cybersecurity awareness. This finding suggests that training programs should focus on inclusivity and universality, ensuring that all employees receive the same foundational knowledge, regardless of age or gender (Negussie, 2023).

5. Perceived Effectiveness and Relevancy of Training:
   While training relevancy showed a weak correlation with perceived effectiveness, it became evident that other factors, such as the interactivity and practical application of training, had a stronger impact on employee perceptions of training value. This finding suggests that relevancy alone is insufficient for effective training; instead, a combination of factors is needed to make training more engaging and impactful (Afolabi, 2024).

5 Conclusion

The research highlights that regular, well-structured cybersecurity training can substantially improve employees' adherence to security protocols in small hotels. By focusing on role-specific training and incorporating interactive elements, hotels can create a more resilient security environment that mitigates risks related to human error, which is often a key vulnerability in cybersecurity. Additionally, the minimal impact of demographic factors on awareness levels supports the development of universal training programs, which can streamline implementation and ensure consistency across the organization (Kahraman et al., 2021).

In conclusion, small hotels can improve their cybersecurity posture through practical, low-cost measures that do not require extensive technological investments. By fostering a security-first culture and implementing optimally-spaced, interactive training programs, SMEs in the hospitality industry can significantly reduce their susceptibility to cyber threats, thereby safeguarding both company and customer data.

6 Recommendations

- Implement Regular, Optimally-Spaced Training:
  Small hotels should establish a structured training schedule, ideally conducting sessions every three to six months. This frequency maximizes employee engagement and knowledge retention, helping them stay vigilant against evolving cybersecurity threats without overwhelming them with information (Afolabi, 2024).

- Enhance Interactivity and Role-Specific Content:
  Training programs should incorporate scenario-based exercises and simulations that mimic real-world cybersecurity threats. Tailoring content to specific roles, such as front-desk staff managing customer data or night-shift employees handling social engineering prevention, makes the training more relevant and applicable (Kahraman et al., 2021).

- Avoid Excessive Training Frequency to Prevent Fatigue:
  Overloading employees with frequent training sessions can lead to disengagement. Instead, prioritize quality over quantity by ensuring that each session is concise, interactive, and relevant. Reinforcing key concepts periodically is more effective than overwhelming employees with constant training (Negussie, 2023).

- Universal, Inclusive Training for Employees:
  Given that age and gender do not significantly impact cybersecurity awareness, it is recommended to provide standardized training for each role within the company. This approach ensures that everyone, regardless of demographic factors, has the foundational knowledge to recognize and respond to cybersecurity threats.

- Incorporate Feedback Mechanisms for Continuous Improvement:
  To adapt training programs to evolving needs, small hotels should regularly collect feedback from employees after each training session. Employee insights can highlight areas for improvement and help management adjust training content to better meet the workforce's needs.

- Explore Third-Party Cybersecurity Training Providers:
  For hotels lacking the resources to develop in-house training programs, third-party providers offer a practical solution. External trainers can provide specialized, cost-effective training that aligns with industry best practices and the specific needs of SMEs in the hospitality sector (Afolabi, 2024).

- Foster a Security-First Culture Across the Organization:
  Beyond formal training, management should actively promote a cybersecurity-focused culture by providing visible support for cybersecurity initiatives, issuing regular reminders about best practices, and integrating security measures into daily workflows to reinforce training objectives. This should be done naturally to avoid overloading employees, ensuring that cybersecurity practices feel like a seamless part of daily responsibilities (Chin, n.d.).

References

Afolabi, J. (2024). Cybersecurity challenges and solutions for small businesses.

Chin, K. (n.d.). Cybersecurity in the hospitality industry [Accessed: 2024-10-29]. https://www.upguard.com/blog/cybersecurity-in-the-hospitality-industry

Kahraman, C., Onar, S. C., Oztaysi, B., & Otay, I. (2021). Modeling humanoid robots mimics using intuitionistic fuzzy sets. In C. Kahraman, S. Cevik Onar, B. Oztaysi, I. U. Sari, S. Cebi, & A. C. Tolga (Eds.), *Intelligent and fuzzy techniques: Smart and innovative solutions* (pp. 339–346). Springer International Publishing.

Negussie, D. (2023). Importance of cybersecurity awareness training for employees in business. *VIDYA - A JOURNAL OF GUJARAT UNIVERSITY*, *2*, 104–107. https://doi.org/10.47413/vidya.v2i2.206