Thematic analysis

📕

Theme 1: Infrequency and Basic Nature of Training

A consistent finding across interviews was the limited frequency of cybersecurity training, often restricted to initial onboarding or annual refreshers. While these sessions effectively covered foundational topics—such as phishing awareness, password management, and basic data protection—employees noted that they were infrequent and insufficient for keeping pace with evolving cyber threats. Advanced cybersecurity practices, such as multi-factor authentication, data encryption, or handling more sophisticated social engineering tactics, were generally not included.

One employee expressed that the infrequent training was “insufficient given how quickly cyber threats change,” highlighting a gap between training schedules and the dynamic nature of cybersecurity risks in the hospitality industry. Participants suggested that without more frequent updates, the knowledge gained from initial training diminished over time, potentially reducing vigilance. This infrequency, as noted by employees, left staff feeling less prepared to respond to complex threats, especially given the sensitivity of guest data in the hospitality environment.

Theme 2: Limited Interactivity and Engagement

Another significant finding was the limited engagement and interactivity within cybersecurity training sessions. Many employees described the sessions as passive, delivered primarily through online videos or brief presentations with little interactive content. This format, which some viewed as a “check-the-box” task, was seen as a hindrance to retaining information and motivation. Respondents frequently expressed a preference for hands-on learning approaches, such as scenario-based simulations or case studies.

One night-shift employee mentioned that “real-life scenarios or quizzes would make training more engaging and relevant” to their specific duties, reflecting a common sentiment among participants. This lack of interactivity, according to the respondents, limited comprehension and reduced the practical applicability of cybersecurity knowledge in daily tasks. Many interviewees indicated that incorporating interactive elements could increase engagement, making cybersecurity practices feel more relevant and actionable within their roles.

Theme 3: Lack of Role-Specific Relevance

The analysis further revealed a disconnect between training content and the unique demands of specific job roles within the hotel. For instance, night-shift employees, who regularly handle security-related tasks, encountered challenges such as managing suspicious phone calls or preventing unauthorized access. Front-desk employees, who often manage sensitive guest information, felt that training could better address best practices for data protection, including Wi-Fi security and identity verification procedures.

One participant described the training as “too generic,” noting that while it covered essential cybersecurity principles, it did not address role-specific challenges. Employees across various roles expressed a desire for training tailored to their responsibilities, suggesting that role-specific content could improve engagement and enhance the practical application of cybersecurity knowledge. By aligning training with job-specific scenarios, small hotels could potentially strengthen staff preparedness to handle the unique cybersecurity threats associated with their particular functions.

Theme 4: Self-Directed Learning and Need for Ongoing Updates

In the absence of regular, structured training, several employees reported engaging in self-directed learning to keep updated on cybersecurity practices. This involved reading online articles, following news on cybersecurity trends, or conducting personal research. However, the effectiveness of this approach varied widely, as it was informal and inconsistent, leading to differing knowledge levels among staff.

One employee shared that they “try to stay informed by reading articles about cybersecurity trends,” but noted challenges in remaining updated without structured support from their employer. This reliance on self-initiated learning pointed to a need for more standardized, ongoing educational efforts within the hotel. Employees suggested that periodic refresher sessions or company-issued updates on emerging threats could reinforce cybersecurity practices and support consistent awareness. Regular management-driven updates, they indicated, would foster a stronger security culture and better prepare staff to handle potential cybersecurity incidents.