Interview Transcript: Cybersecurity Practices in Small Hotels(5)

Respondent:

We typically have training sessions **once or twice a year**, based on updates to our policies. It's not as frequent as I'd expect, especially given how quickly cyber threats change. There have also been occasional **refresher sessions**, but they're relatively short. The training provides a good foundation for handling basic cybersecurity threats, like recognizing phishing attempts or following secure password protocols. However, it's more focused on **surface-level issues** and doesn't fully prepare us for more complex or sophisticated threats, especially those related to larger cyberattacks.

The training is delivered through a mix of **online modules and in-person workshops**. The online modules are self-paced, while the in-person workshops are more interactive and allow us to ask questions and get immediate feedback from the IT team. Overall, the training was easy to follow.

Highlighted for thematic analysis: Infrequency of training, focus on basic issues, mixed format with online and in-person workshops.

The online modules are user-friendly, and the in-person workshops provided examples that clarified complex topics. However, some of the more technical parts, especially around data encryption and advanced cyber threats, could have been explained in simpler terms. As a **night receptionist**, I handle sensitive guest information like payment details, so sections on data protection and phishing were particularly relevant. But certain parts felt geared toward IT staff rather than frontline employees like myself.

One area that could have been covered better is **social engineering attacks**. While we discussed phishing emails, there wasn't much focus on tactics like

phone-based scams or impersonation attempts, which are also risks in our role. We do get occasional refreshers, but they're not as frequent as they should be.

Highlighted for thematic analysis: Job relevance, need for simpler explanations on technical topics, lack of social engineering training.

In an ideal scenario, we'd have more frequent training updates since cyber threats are constantly evolving. Most information I receive comes from **AI bulletins or email updates** from the hotel's IT department. I also try to stay informed by reading articles and news about cybersecurity trends on my own time. During training, I was fairly engaged, especially in the in-person workshops, where we could participate in quizzes and group discussions. However, the online modules were more static, making it harder to stay engaged.

Highlighted for thematic analysis: Self-directed learning, varied engagement levels between online and in-person formats.

I feel motivated to follow cybersecurity practices because I know that small mistakes can lead to serious security breaches, especially when handling guest data. The training emphasized the consequences of not following best practices, which helped underline the importance of vigilance. One challenge I faced was understanding some of the more technical aspects, like **data encryption** and **malware functionality**. I also think the training could include more **real-world scenarios**, which would make it easier to relate. Interactive components like **simulations of cybersecurity incidents** could make training more engaging and relevant.

Additionally, shorter and more frequent training sessions would help reinforce key concepts and keep cybersecurity top of mind.

Highlighted for thematic analysis: Motivation due to job impact, difficulty with technical content, need for real-world scenarios and simulations.

I haven't personally encountered any major cybersecurity issues, but I have received **suspicious emails** that were likely phishing attempts. Thanks to the training, I recognized the red flags and reported them to IT before any potential damage could occur. After this incident, IT sent out a company-wide reminder on spotting phishing attempts and encouraged employees to stay vigilant. However, no additional formal training was provided following the incident.

I would suggest providing more frequent refreshers and making the training more **scenario-based** with practical examples on how cyber threats impact our specific roles. Simplifying technical aspects would also make the training more accessible to non-technical staff. Regular training would keep employees more informed about the latest threats and best practices, reinforcing the importance of vigilance and helping to prevent common errors, such as falling for phishing scams or mishandling sensitive data.

Highlighted for thematic analysis: Practical application in phishing prevention, need for simplified, scenario-based training.