

Is my Accommodation Programme as secure as it should be?

According to annual surveys conducted by the Institute of Travel Management, duty of care remains the top priority for travel managers which is no surprise.

Accommodation options have the highest potential to be a “weak link” in meeting these duty of care responsibilities in corporate travel programming. To mitigate Travel Manager liability, extreme care should be taken to ensure the risks and concerns of travellers regarding their security are addressed:

89% • of hotel guests rank security as their first concern when travelling (Travelzoo 2017)

65% • of corporate travel managers said their companies' attention to travel risk management has increased over the past 3 years (BTN 2017)

64% • of travel security professionals believe the risks facing travellers have increased (Ipsos-Mori 2017)

50% • of corporate travel managers said business travellers have expressed increasing anxiety levels about safety and security during the past three years (BTN 2017)

48% • of business travellers said they would consider not travelling abroad for work if it took them to a location they considered unsafe (SAP Concur 2018)

According to the 2019 Verizon Data Breach Investigations Report, point of sale intrusions, web applications and crimeware patterns represent 93% of all data breaches within the Accommodation sector, the most prevalent environment for cyber breaches. Travellers are exposed to their highest risk of being cyber-attacked when staying in properties that do not have robust and highly managed security protocols in place to monitor and remove the use of bogus networks set up within their environment. Corporate reputational damage will result from such attacks.

Travel Managers have a responsibility to mitigate risk and unfortunately the current accommodation security landscape is proving to be an area of concern which requires greater management due to:

- Hotels and other venues largely seen as easy targets with big impacts and easy rewards
- The open-access nature of hotel buildings with frequent visitor traffic patterns
- Often an uncontrolled environment providing a data rich playground for cyber-criminals

Several travel managers have already included security questions in their RFPs, but it is extremely difficult for travellers and travel risk managers to assess whether the preventative measures are actually in place, effective and maintained. Most of the tender process focuses on comfort, facilities and service. Standards and security capabilities in hotels vary enormously and can be heavily influenced by hotel ownership structures and can largely be self-regulating when it comes to the protection of guests. Also, the travel risk manager and security team are the ones who are in the firing line when there are issues at those properties, from a due diligence perspective.

Due to the increased risk of incidents, travel insurance companies are taking a greater interest in the activities undertaken by corporates to help reduce claims. By demonstrating a desire to mitigate risk, not only does the Travel Manager stay the right side of the Corporate Manslaughter/Homicide Act of 2007, which has a potential for personal liability, but a corporate saving on travel insurance premiums can also be explored.

The requirement for accommodation providers to meet security standards is currently not regulated and thus trust is a key requirement they will meet their duty of care standards. There are properties which take this commitment extremely seriously but the more complex the structure of property ownership, the harder it is to ensure all standards are consistently being met equally across their network. This is where the opportunity for risk significantly increases.

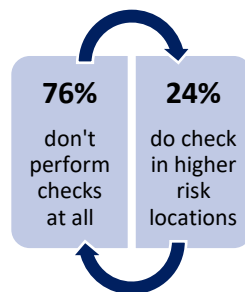
Asking the right questions and obtaining confirmation from every property on your programme, which is evidenced via audit, assures your approach to risk mitigation is regarded as best practice. With the launch of ISO31030 standard in early 2020 to regulate travel risk management standards, now is the time to be speaking to your accommodation providers to encourage them to commence the process to obtain the only independent security solution which has an Ofqual (UK Government Standards) accreditation from SFJ Awards and that is delivered by Global Secure Accreditation.

The Global Secure assessment covers over 120 security components grouped in the following main security headings:

1. Strategic Planning	4. Physical and Technical Security
2. Policies and Procedures	5. Access Control Measures
3. Perimeter Security	6. Workforce

The audit is risk based and so an independent threat and risk profile determines the levels and type of security that must be evidenced by the hotel based on physical, geopolitical, socio-economic and other assessment criteria.

Ipsos MORI Global Business Resilience Trends Watch 2019



* Accommodation security checks

Travel managers are encouraged to engage their accommodation providers to support this programme of risk mitigation and seek accreditation to provide independent and robust security assurance and secure their future opportunity to work within your corporate programme, especially if access to security support is not available in all locations. There is no cost to corporates to sign up to this programme of risk mitigation.

Having done this, you can answer the opening question positively.