HotelBusiness
The number 1 ABC certified trade magazine for the hotel industry across the UK

WHO OWNS CYBER SECURITY IN A HOTEL FRANCHISE?

HOTEL BUSINESS 19 DECEMBER 2016

By Geoff Milton, security strategist, ShieldQ

Numerous, high-profile breaches over the last couple years have raised concerns over whether the hotel industry is serious about cyber security. The last 12 months alone have seen multiple data breaches in some of the biggest chains, including independent HEI Hotels, which operates hotels for the likes of Marriott, Starwood and Hyatt[]. Unlike other industries, the hotel industry has a very specific set of challenges, due to the business model in which many chains operate.

Whenever a large or well-known hotel chain becomes the target of a publicised breach, it's the brand that takes the reputation hit, even though the breach might originate from the franchisee's property or property management company. Actual liability, however, depends on the contract between the brand and franchisee, but may vary considerably in the way they account for responsibility. In addition, most franchisees have multiple properties, each with their own brands and corresponding contracts which, more often than not, differ from another franchise's.

The question that needs to be addressed is, "Who is responsible for the cyber security in a hotel franchise?" Is it the hotel brand, the property management company, the franchisee? Or is it all three?

Contract suitability in light of the GDPR

Cyber-attacks are becoming increasingly sophisticated, using methods and techniques designed to evade detection. The problem is, many of today's hotel franchise contracts fail to take these complex security challenges into consideration. Given that headline-grabbing remote payment card breaches have shifted from large retailers in 2014 to hotels chains in 2015 (according to the 2016 Verizon Data Breach Report), these chains and their franchisees need to be asking whether these contracts are fit for purpose.

This question takes on more importance with the looming European Union General Data Protection Regulation (GDPR) – which comes into effect in 2018 – where companies can face fines of up to 4% of global turnover if they fail to protect personally identifiable information (PII).

Who would pay the penalty if such an incident occurred?

As Philip Lieberman, president of Lieberman Software recently stated, the current business model of hotels and their franchisees does not include cyber security as one of the deliverables provided to their licensees[ ]. The problem is, franchisees are not security experts, yet they carry huge responsibility for protecting brand reputation.

Owning up to responsibility

Many hotel owners as individuals often don't consider the impact of data security, because they themselves don't directly collect or store PII; they engage managers and brands to handle these activities through reservation systems. However, owners must recognise that the business has a legal obligation to protect this information. Most hotel franchise agreements also state that the hotel – and its owners – will be responsible for defending the franchisor, even if the data breach originates from their reservation system. Likewise, independent properties using third-party reservation systems will almost always hold the owner responsible for a breach[ ].

As you can see, there doesn't seem to be a definitive answer as to who is responsible for cyber security in a hotel franchise, but there are ways in which a hotel owner can help minimise the cost and damage, should they become a victim of an attack. The use of cyber insurance, for example, is widely increasing and comes in a wide variety of forms and costs. Hotel franchisees (and their owners) should look at themselves as leaders in the fight for cyber security. They already take responsibility for the physical safety and security of their guests, so why not their data, too?

Solutions available on the market today offload the responsibility for data compliance to a third party. Engaging with providers offering compliant data management environments is one way to reduce data breach risk. In turn, franchisors and their corporate security teams should take responsibility for fully explaining the threats and contractual obligations of franchisees. They should provide incentives and a clear direction on how to solve all security issues in all areas of the business, not just those that are perceived to be the biggest risk.