Tech-Savvy Innovative Hotels Are More Vulnerable to Data Breaches

The race to become the most innovated and tech-savvy hotel is on. Hotels have increasingly begun working with technology companies to offer more innovative and enhanced guest experiences. Guests at many hotels can now bypass the need to go to the front desk by using their mobile devices to select a room, check-in, receive texts when their room is ready, and even unlock the door to their room. Guests can also customize their stay by requesting items, ordering room service, planning activities, or purchasing upgrades. Everything a guest may want is only a few clicks or taps away, and soon, the data collected by these programs will allow hotel operators to anticipate guests' requests and needs.

These services along with public WiFi networks, data-sharing with OTAs, smartphone key cards, and other interconnected systems makes the hospitality industry particularly vulnerable to a data breach. According to Trustwave's 2016 Global Security Report, the hospitality industry accounted for the second largest share of data breach incidents by industry at 14% of the incidences investigated by Trustwave and was followed by the food and beverage industry at 10%.[1] The amount of data hotel operators can gather and store about their guest can be a double edged sword. Hoteliers should be aware of potential complications that come with these added conveniences, such as the responsibility to protect their guests' personal information, as well as the physical security of the guests' rooms from a privacy event or data breach.

A privacy event or data breach triggers certain "clean up" protocol, regardless of the cause or the materiality of the breach. There are two aspects to any clean up. One side is the legal compliance with the various laws and regulations that are triggered and the other side is the public relations management. The 2016 Ponemon Cost of Data Breach Study: United States (sponsored by IBM) found that the average cost per lost or stolen record in the United States is $221 and the average total cost of a single data breach was $7.01 million in the United States.[2] A "breach coach," who is often a lawyer, can help determine if there was a breach, what needs to be done to comply with the legal regulations, what forensic investigation is needed, and what else needs to be done to best manage any potential liability and public relations.

Cyber security laws are constantly evolving, but for the foreseeable future, these laws will likely be constantly behind the development of new technology. Therefore, it is important for hoteliers to be forward thinking and prepare for changes to the laws in the future. Currently, each state, territory, and the District of Columbia varies on its notification and reporting requirements, as well as the fines and penalties related to a breach. Notification to the affected individual must be made in compliance with the laws in the state in which the affected individual resides. A single hotel could be exposed to more than fifty different notice requirements, more than fifty different state actions by more than fifty different state regulators, and more than fifty different fines and penalties.[3]

In part one of this two-part article, Samantha Ahuja Morris, partner in the Hospitality and Commercial Real Estate Development & Finance practices, at Manning & Martin, LLP and Molly Kacheris, associate in Morris, Martin & Manning, LLP's Commercial Real Estate Development and Finance and Hospitality practices, discuss how hotel owners and operators can limit the amount of unknown risk and liability, with PCI-DSS compliance and by implementing other preventative measures. In part two, they will discuss implementing contract provisions that establish each party's responsibilities and prescribes who bears the risk if there is a breach, and the purchasing of cyber liability coverage.

PCI Compliance

PCI Security Standards Council created the Payment Card Industry Data Security Standards (PCI-DSS). The PCI-DSS Requirements and Security Assessment Procedures published by the PCI Security Standards Council can be found at www.pcisecuritystandards.org.[4] Using these guidelines, hotel owners and operators should implement a secure network and security policies and then monitor and test the network and policies to determine if the hotel is vulnerable to a breach.

The goal of these standards is to protect consumers at the point of sale and the storage of consumers' confidential information. PCI-DSS is a standard that all business must follow when processing, transmitting or storing customer credit or debit card data. PCI-DSS compliance is dictated by the Security Standards Council, but is enforced by the payment card companies. If businesses do not comply or fail to remedy a security issue, they risk fines from the payment card companies and possible prohibition on use of their cards.

Hotel operators should be mindful of the data they are collecting and segregate sensitive data so that only necessary employees have access to the relevant data. For example, a human resources employee would have access to all classes of employment related data, but only "public" financial data. Hotel owners and operators should also promptly and securely destroy outdated data.

Creation of separate networks for each aspect of the hotel is a good way to prevent wide-spread access to all networks from access gain to the more vulnerable networks. Hotels could use a dedicated network for reservation, payment cards, and other highly sensitive information. A second network could be used for email and social media, which are highly vulnerable to a breach. Doing so would prevent a phishing email or an infected social media website from compromising the guests' payment accounts.

Additionally, the use of smartphones as room keys may require a separate Wi-Fi network. The room keys would likely use Near Field Communications (NFC) technology to unlock the doors, which, similar to radio-frequency indemnification (RFID) technology, can transfer small amounts of data between two devices that are a few inches from each other. The possible risks this new technology creates are still unknown.

Hoteliers should also manage the relationship they have with third party vendors. Outsourcing of business tasks leads to increased amounts of data sharing among business so that the third party vendors can adequately provide their services. Attackers frequently exploit third party vendors' or contractors' networks to access the data of the larger companies. If third party vendors collect, store, process, or transmit the data of your business or your guests, be sure to investigate and determine if their privacy and security policies are adequate. It is important to delineate your vendor's specific obligations (such as tracking who as access to your files and alerting you when passwords change), rather than generically stating that the "vendor shall comply with all applicable laws." This ambiguity can be resolved by specifically allocating this risk using express contract clauses.

Samantha Ahuja and Molly Kacheris with Morris, Manning & Martin represent owners, operators and developers of hotels with a focus on hotel acquisitions, operations, development and finance, hotel management agreements, licensing agreements, and commercial real estate acquisitions and sales. They can be reached at sahuja@mmmlaw.com and mKacheris@mmmlaw.com.

---

[1] https://www.trustwave.com/Resources/Trustwave-Blog/Introducing-the-2016-Trustwave-Global-Security-Report/
[2] http://www-03.ibm.com/security/data-breach/
[3] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[4] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1487008020201