Hotel Cybersecurity: Protecting your guests and your property from vendor data breaches

19 July 2017

Click here for the latest articles on Data Technology, Privacy & Security.

Hotels rely on third-party vendors to help run their properties efficiently, and often must give them access to sensitive guest data. This leaves hotels vulnerable to cyber attacks; they’re only as secure as their vendors are, and may find themselves directly liable for a data breach. My partner Bob Braun, senior member of JMBM’s Global Hospitality Group® and co-chair of JMBM’s Cybersecurity and Privacy Group, discusses recent hotel cybersecurity breaches and how hotel owners can protect themselves.

Hotel data breaches
It’s not you, it’s your “friends”
by Robert E. Braun

July was another notable month for hotel data breaches – on a single day, several well-known hotel brands and managers, including Four Seasons, Trump Hotels, Hard Rock Hotels & Casinos and Loews Hotels all announced that customer data may have been compromised as a result of a security failure. Each of the incidents is related to Sabre Hospitality Solutions’ credit card data breach in its SynXis hotel-reservations system, which Sabre first announced in a quarterly filing with the Securities and Exchange Commission on May 17. Based on Sabre’s investigation, Sabre announced that the breach was contained to “a limited subset of hotel reservations,” but the incident did allow an unauthorized party to access cardholder names, payment card numbers, card expiration dates, card security codes for some, and, in some cases, guest name, email, phone number and address.

Moreover, the duration of the breach was long quite long. Sabre’s investigation determined that the unauthorized party first obtained access to payment card and other reservation information on August 10, 2016, and the last access to payment card information was on March 9, 2017. The hackers had potential access for seven months.

Hotel owners and consumers are, unfortunately, common victims of security breaches – all of the major hotel brands and managers have been breached, often multiple times. In analyzing the breaches, there is something that is common to almost all incidents: the vulnerability was not with a hotel, its manager or brand, but with a vendor.

Hotels are not alone, of course in relying on vendors. Companies in other high threat industries like finance, retail, and healthcare regularly work with third party vendors, and these third parties commonly have access to their clients’ systems and may share or store clients’ sensitive and highly-valued data. But this Sabre breach (and those of the past several years) shows us that no matter how well-protected a hotel is from a direct cyberattack, its networks and data may still be easily accessed through third parties with weaker cybersecurity protections. In one of the most famous (or infamous) breaches, the 2013 breach of Target, cybercriminals were able to steal the retailer’s sensitive data by accessing its
systems with credentials stolen from a vendor responsible for Target’s HVAC systems. Similarly, in 2017, thieves stole Netflix’s “Orange is the New Black” episodes from an audio post-production company, not from Netflix itself.

The typical hotel management or franchise agreement requires the owner to abide by or adopt data security policies and procedures in conformance with the brand’s or manager’s standards and to comply with data security laws and regulations. As a result, even where an incident is the result of the manager’s or brand’s failure to adopt or maintain appropriate standards, the owner will likely be directly liable for a breach, and may be obligated to indemnify the brand or manager for any claims arising from a breach.

Hotel owners are at a particular disadvantage compared to other companies, since hotel brands and managers typically select vendors, like Sabre, for multiple properties and often for an entire brand. Hotel owners may have little, if any say, in the vendor, the terms of engagement, and the impact of a breach. However, under the typical hotel management or franchise agreement, the hotel owner is required to bear the cost of a breach, whether in terms of direct costs (including notifying potential victims and the increased cost of cyberliability insurance) and the indirect cost of diminished trust in the hotel.

While managers and brands are reluctant to cede authority to owners, owners should take active steps to protect themselves and their properties:

1. Review data security policies and procedures critically, and require changes where the policies don’t reflect current laws and regulations and, most importantly, current cyber-threats. Training programs should include a strong cybersecurity and monitoring for implementation and effectiveness. Most incidents can be traced to human error or malicious intent, not solely to technical systems.
2. Require brands and managers to impose security requirements on vendors and to ensure that vendors take responsibility for the cost of a breach.
3. Analyze cybersecurity policies to confirm that they adequately cover direct and third party costs of breaches. Since insurance is often one area where a hotel owner has greater control, it can be used as a lever to create a more secure environment.
4. Require that brands and managers develop and test effective backup systems; while theft of data is expensive and embarrassing, newer strains of ransomware, wiperware, and fileless malware have the ability to destroy business records, and only a functional backup system can protect the hotel and its business.

JMBM’s Global Hospitality Group® works with the JMBM Cybersecurity and Privacy Group to help clients analyze risk and develop response plans and other procedures to reduce vulnerability to data breaches. For more information, contact Bob Braun at rbraun@jmbm.com.

Other information about cybersecurity issues

If this article was of interest, you may also wish to read other articles on “Data Technology, Privacy & Security,” which include the following articles:

Hotel Cybersecurity: What can happen when hackers strike?
Hotel Cybersecurity: Closing the doors before the horses leave the barn

What every hotel owner (and operator) needs to know about “data security” after the Wyndham case

What the Target data security breaches mean for hoteliers

Cyber Security Alert: How to protect your proprietary information from employees

Hotel Lawyer Privacy Alert: Do your hotel mobile apps comply with new interpretations of online privacy rules?

Hotel Liability for Guest Information — What you need to know and how to avoid liability.

Losing the expectation of privacy bit by bit, byte by byte.

Dodd-Frank Act presents Hotels with decisions on credit and debit card charges.

Bob Braun is a Senior Member of JMBM’s Global Hospitality Group® and is Co-Chair of the Firm’s Cybersecurity & Privacy Group. Bob has more than 20 years experience in representing hotel owners and developers in their contracts, relationships and disputes with hotel managers, licensors, franchisors and brands, and has negotiated hundreds of hotel management and franchise agreements. His practice includes experience with virtually every significant hotel brand and manager.

Bob also advises clients on condo hotel securities issues and many transactional matters, including entity formation, financing, and joint ventures, and works with companies on their data technology, privacy and security matters. These include software licensing, cloud computing, e-commerce, data processing and outsourcing agreements for the hospitality industry.

In addition, Bob is a frequent lecturer as an expert in technology, privacy and data security issues, and is one of only two attorneys in the 2015 listing of SuperLawyers to be recognized for expertise in Information Technology. Bob is on the Advisory Board of the Information Systems Security Association, Los Angeles chapter, and a member of the International Association of Privacy Professionals. Contact Bob Braun at 310.785.5331 or rbraun@jmbm.com.

This is Jim Butler, author of www.HotelLawBlog.com and hotel lawyer, signing off. Please contact us if you would like to discuss any issues or development that affect your hotel interests. We would like to see if our experience might help you create value or avoid unnecessary pitfalls. Who’s your hotel lawyer?
Jim Butler is a founding partner of JMBM and JMBM’s Global Hospitality Group® which provides business and legal advice to hotel owners, developers and investors. This advice covers hotel purchase, sale, development, financing, franchise, management, labor & employment, litigation, ADA, IP, EB-5 matters any many other areas.

Jim is recognized as one of the top hotel lawyers in the world and has led the Global Hospitality Group® in more than $87 billion of hotel transactions and more than 3,900 hotel properties located around the globe.

Jim’s group has advised on more than 100 EB-5 projects, closed more than $1.5 billion of EB-5 financing, and sourced more than half of that for our clients.

Contact Jim at +1-310.201-3526 or JButler@jmbm.com