Cyberattacks on Hotels — What Should Hotel Owners and Operators Do?

22 January 2018

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

Protecting guests’ information (and employees’ information) from hackers is one of the biggest business challenges faced by hotel owners today. Data breaches can result in loss of reputation and loss of revenue, and can trigger costly lawsuits and government investigations.

In his earlier article, Not Just Heads in Beds – Cybersecurity for Hotel Owners, my partner Robert Braun reminds hotel owners that they are generally required to indemnify brands and managers for costs incurred, which could include the cost of a data breach. Now, in his article below, he discusses why hotel data breaches are prevalent and what owners need to do to create a secure data environment for the properties they own.

Cyberattacks on Hotels — What Should Hotel Owners and Operators Do?

by

Robert E. Braun, Hotel Lawyer

This article was originally published by Hotel Business Review and is reprinted with permission from www.hotelexecutive.com.

Almost as soon as there were data breaches, hotels became a prime target of hackers, and the hospitality industry has consistently been one of the most commonly targeted businesses. Since 2010, hotel properties ranging from major multinational corporations to single location hotels have been impacted.

The recent report that Hyatt Hotels was a victim for the second time in as many years has raised more concerns about the industry’s ability to address cybersecurity. While consumers are so used to receiving breach notices that “breach fatigue” has set in, the second successful attack on Hyatt is sure to raise the eyebrows of regulators, plaintiffs’ lawyers, and guests. The data breach will affect the loyalty, trust and consumer perception of all Hyatt Hotels guests. So how can hotels prove to guests that they are safe and trustworthy?

“While the company claims that it has implemented additional security measures to strengthen the security of its systems, no explanation was given as to why these additional measures were not implemented after the first attack,” said Robert Cattanach of Dorsey & Whitney. “Estimates of actual harm have yet to be provided, which is typically the weak spot of any attempted class action, but the liability exposure seems problematic regardless.”

Hyatt is in no way alone. On November 2, 2017, the BBC reported that Hilton was fined $700,000 for "mishandling" two data breaches in 2014 and 2015. The attorneys general of New York and Vermont said Hilton took too long to inform their guests about the breaches and the hotels "lacked adequate security measures." Hilton discovered the first of the two breaches in February 2015 and the second in July 2015, according to the article, but the company only went public with the breaches in November 2015. The company has said there is no evidence any of the data accessed was stolen, but the
attorneys general said the tools used in the data breaches made it impossible to determine what was done.  Read More

**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](http://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