Hotel Cybersecurity: What can happen when hackers strike?

1 February 2017

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

Theft of confidential data by hackers is a major threat to businesses worldwide and the hotel industry is no exception. Hoteliers remain vulnerable to hackers seeking confidential information such as guests’ credit card data and employees’ personal information. They are also vulnerable in other ways. In a recent hotel breach, the hackers did not go after confidential data, but rather sought a ransom payment after taking control of the hotel’s technology. My partner Bob Braun, senior member of JMBM’s Global Hospitality Group® and co-chair of JMBM’s Cybersecurity and Privacy Group, describes what happened, and shares what hotels can do in response to such threats.

**Hotels and Ransomware — Something Special**

**by**

Robert E. Braun

Last year, at the Global Hospitality Group’s Meet the Money™ Conference, I participated in a panel on Cybersecurity and we discussed how cybersecurity issues affect the hotel industry. One of the comments was that hotels, more than most private industries, have to take into account the kind of physical harm that might be done by a hacker. We noted that not only are guest information systems targets, but also the life and safety systems – HVAC, elevators, electricity and so on. We concluded that while financial theft could impact a hotel and its reputation, a hack of the physical structure of a business could put the hotel out of business.

**Locked Out**

Our discussion turned out to be prescient when, this week, Romantik Seehotel Jaegerwirt, in the Austrian Alps, had their systems frozen by hackers, which resulted in the complete shutdown of hotel computers.

The 111-year-old hotel had already been targeted by hackers twice. This time, however, the hackers breached the key card system, made it impossible for guests to enter their rooms and prevented the front desk from reprogramming cards.

The hackers demanded €1500 in Bitcoin, promising that control of the key card system and room locks would be returned. Management of the hotel, fully occupied at the beginning of the winter season, chose to pay the ransom, rather than attempt a solution that could have taken significant time and harmed their 180 guests.

The story could have been worse; once a hacker breaches a system, the system remains open until the vulnerability is eliminated. In this case, the hotel took the precaution of seeking and remediating a backdoor the hackers left (which they tried to exploit, almost immediately) and was able to secure their systems.

**The Threat to Hotels**
We have pointed out before that hotels are particular targets of hackers. During 2015 and 2016, every major hotel company was breached. In each case, however, hackers attacked hotel point of sale systems for the straightforward goal of obtaining personal information. This, however, may be the first case where hackers threatened the safety of guests, something much more important. After all, guest safety is paramount, and threats to safety can overcome every other achievement.

Moreover, hotels are complex businesses with overlapping and interconnected systems. Thus, finding a way into one system can allow a bad actor to access other parts of the hotel, giving them the opportunity to demand payment for protection. Hotel owners and operators should be aware that ransomware is increasingly popular because it provides for almost immediate return on a hacker’s “investment.” Rather than selling personal information, which rapidly loses value, the use of ransomware gains the hacker an immediate return. Moreover, as with the Romantik Seehotel Jaegerwirt, hackers will now know the hotel’s vulnerability, or leave a backdoor, allowing them to shake down the same institution multiple times.

**What Can Hotels Do**

Hotels need to take the same steps that other business take to achieve data security:

- **Analyze risk.** Each business is different, and each business needs to identify the risks it is willing to take, and how it can neutralize the other risks. For a hotel, this can include decoupling systems – preventing, for example, the key card system from access through the hotel’s website – or preparing for workarounds. In the case of the Romantik Seehotel Jaegerwirt, the decision has been made to include physical keys, allowing a manual override of the system.
- **Train Personnel.** Virtually every breach is the result of a human act, whether an error or malicious act. Training personnel to identify risks and avoid them is one of the most effective steps to reduce cyber risk.
- **Plan for the breach.** No matter what technical or personnel prevention is taken, every system capable of authorized access is vulnerable to unauthorized access. When that happens, it is too late to design the response playbook. Hotels, like other businesses, have to design, implement and test response plans, and update them regularly.

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: 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. Why don’t you give us a call (or send an email) and let us know what you working on? We would like to see if our experience might help you create value or avoid unnecessary pitfalls. Who’s your hotel lawyer?

Our Perspective. We represent hotel owners, developers and investors. We have helped our clients find business and legal solutions for more than $87 billion of hotel transactions, involving more than 3,900 properties all over the world. We bring this experience to any hotel project — big or small. Let’s explore how it might work for you. For more information, please contact Jim Butler at jbutler@jmbm.com or +1 (310) 201-3526.