Published by *Hospitality Law360* on August 11, 2015. Also ran in *Insurance Law360* and *Privacy Law360*.

The Limits Of Insurance In Managing Hotel Cyberrisk

--By William M. Bosch and *Anthony F. Cavanaugh, Arnold & Porter LLP*

Law360, New York (August 11, 2015, 4:24 PM ET) -- It doesn't require too great a leap to imagine a scenario where hackers infect computers in electricity generator control rooms with malware, causing a number of states across the United States to lose power and affecting millions of people and numerous businesses. That's precisely what Lloyd's of London and the University of Cambridge's Centre for Risk Studies contemplated in a July 2015 report examining the insurance implications of a widespread cyberattack affecting the eastern United States. The Lloyds report predicted the losses resulting from such an attack could trigger $70 billion in insurance claims.[1] Lloyd's separately has expressed concern about underwriting cyberrisks, noting that "without proper controls there exists a material risk of a dangerous aggregation of exposure in the market."[2]

The cyberthreats and aggregation risks contemplated by the Lloyd's report are clearly concerning to the hospitality industry. These risks go beyond privacy breaches by hackers, which already have ensnared companies like Wyndham and White Lodging, among others. The losses caused by a massive power outage alone extend beyond business losses and property damage to personal injury and loss of consumer confidence. And given the number of hotel companies that have centralized IT, accounting and procurement functions, by way of example, the "aggregation risks" noted by Lloyd's seem especially problematic, as an attack on one management company could affect hundreds of hotels.

Aggregation Risk in the Hospitality Industry

Aggregation risk in the context of a cyberattack arises when there are a number of similarly situated entities connected to each other more frequently and in more advanced ways than ever before, potentially posing risk of loss attributable to the same or overlapping incident. Insurance companies are concerned about the potential for a dangerous aggregation of insurance claims resulting from a single cyber event that affects a large number of these interconnected entities. Branded hotels give rise to aggregation risks, because the company managing or franchising an individual hotel typically provides centralized services at a corporate (that is, branded hotel company) level. For example, the hotels managed under one brand often share networked accounting and IT systems that are maintained and operated at the corporate or "brand" level. A cyberattack affecting these computer systems could have a devastating ripple effect on all of the hotels within the system. An entire hotel chain could lose access to its reservations, operations and point of sale systems, or could suffer theft of extensive amounts of sensitive personal data (including financial information and, for some chains, unique personal information about how guests spend their time and money) — exposing hotel management companies, franchises and hotel owners to a cascade of losses and claims.

Attacks on the power grid clearly are not the only aggregation risk confronting the hospitality industry, especially given the data breach and related privacy concerns already manifesting themselves. The aggregation risks posed by hackers is more than a hypothetical area of concern, as manifested by the experiences of Wyndham, White Lodging and others. As is typical in the industry, Wyndham operates a brand-level property management system that connects to the computers at each of the individual hotels it manages. This system "handles reservations ... and ... payment card transactions" and "store[s] personal information about consumers, including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates and security codes."[3] On three occasions between 2008 and 2010, hackers gained unauthorized access into Wyndham's property management system, compromising payment-card information that Wyndham had collected from customers across its managed hotels. These breaches at the brand level could expose not only the brand, but all Wyndham hotel owners and franchisees to losses (including investigation and remediation costs) and to claims by customers and other parties whose data was compromised.

The recent cyberattacks at hotels operated by White Lodging Services demonstrate the risk is not unique to any brand, but is a threat targeting the industry generally. In 2014 and 2015, White Lodging reported two separate breaches of its point-of-sales systems at a number of its managed hotels.[4] Before White Lodging acknowledged the breach, the story was broken on a website maintained by a private computer security investigator, which noted that multiple sources in the banking industry detected a pattern of credit card fraud at specific Marriott hotels, which all were managed by White Lodging. Although White Lodging reported that the breaches were contained at the affected hotels, the clear inference is that the network intrusion affected the management company's network. Whether a hacker uses the property-level systems to gain access to the brand-level systems, or vice versa, the security of each hotel's data (and the risk of loss) is only as strong as the weakest link in the chain.

Additional Risks to Branded Hotel Owners

Who ultimately bears financial responsibility for losses caused by cyberattacks remains to be seen. Cyberrisks can be addressed through prudent insurance coverage, but this is not necessarily the solution to the problem hotel owners may think it is. It is unclear whether losses caused by a cyberattack would be covered by traditional insurance policies. The Lloyd's report found that, with respect to traditional insurance policies, there are a number of areas where "there could be significant ambiguity around how coverage will be interpreted and whether claims could reasonably be expected to be successful or denied." The Lloyd's report also suggests that specialized cyber policies may not cover as much as expected by the policyholder.

The market for cyberrisk insurance continues to mature. But as the insurance industry evaluates how to underwrite these policies given the aforementioned aggregation issues, it is clear that the hotel industry needs to more closely evaluate the role and limits of insurance in managing risk. Clearly, there is an important and perhaps primary role to be played by hotel management companies, who are often delegated the authority to manage the systems that give rise to the risks and create the aggregation issues that are going to affect the insurance market.

Hotel owners perhaps are at the greatest risk, given their lack of visibility into and limited control over the growing threat of cyberattacks. Some managers consider the insurance policies procured at the brand level to be proprietary and will not share the policy with owners, making it difficult for owners to fully understand the terms, including the all important coverage limits and exclusions. Policies written to cover the costs of investigation and remediation sometimes are triggered by the location of the network intrusion, which could leave individual hotels (and owners) in a grey zone — and potentially without coverage. And as cyberattacks materialize, whether in the nature contemplated by the Lloyd's report or consistent with the privacy breaches already experienced by several hotel companies, parties increasingly will be looking at their contracts, including indemnification clauses, to determine where those risks are properly allocated. Since this is an emerging issue, most management agreements are silent on indemnification or allocation of risk resulting from a cyberattack.

These insurance risks to hotel owners are compounded by a number of other factors specific to the hotel industry. For instance, several hotel management companies operate their own, captive insurance entities. A broad-based attack, such as the one envisioned by Lloyd's, could generate a substantial number of claims which could quickly exhaust self-retention limits and overload the claims process for these captive insurers. It may also be the case that the captive entities are not sufficiently capitalized to handle the number of insurance claims following a brand-level cyberattack.

Further compounding the risk to hotel owners is the fact that owners often do not have visibility into whether hotel management companies are using best practices before or after a loss event occurs. Most hotel management agreements require the manager to provide some level of transparency. This often is set forth in

the management agreement's “books and records” provision, which requires the manager to maintain and make available information “relating to the operation of the hotel.” Some managers narrowly interpret these provisions to only allow access to information that is specific to the owner’s hotel. Under this approach, the manager takes the position that the hotel owner is not entitled to any information relating to, by way of illustration, corporate-level programs or systems imposed on the hotel and paid for by the owner. Other managers contend that they are entitled to withhold information on these systems on the grounds that they are proprietary to the management company.

This lack of transparency raises several concerns, which if not addressed directly are likely to lead to disputes. Hotel owners often do not have control of the information regarding management company-level systems and, thus, do not have the ability to independently investigate cyberattacks when they occur. This puts owners in a difficult position. Even though owners may have been charged for the development of management-company systems which may expose owners to greater cyberrisks (knowingly or not), owners have little control or information on how management companies investigate and prevent these attacks. The risk is already materializing that some management companies will take advantage of their access to and control over information to pass through as “operating expenses” the costs incurred to investigate and remediate network intrusions that happened at the brand management level.

Conclusion

The threat of a cyberattack is very real and could have a devastating effect on the hospitality industry. To mitigate the damage from a cyberattack and to ensure proper insurance coverage, hotel owners should scrutinize their traditional insurance policies and any special cyberinsurance policies they possess. Owners should discuss these policies and exclusions with their insurers and brokers, so that there is no ambiguity as to what is covered and what is not. Most importantly, it’s time to add language to management agreements delegating the responsibility to manage and insure these newly emerging cyberrisks. In our view, this responsibility, and the costs associated with intrusions, typically will be best allocated to the operator. Managing risk is one of their important duties, and management companies — with their superior access to information and control over the systems giving rise to these risks — are in a better position to take on this growing and unnerving challenge.

William Bosch is a partner and Anthony Cavanaugh is counsel in Arnold & Porter's Washington, D.C., office.

[1] New Lloyds Study Highlights Wide Ranging Implications of Cyber Attacks
[2] Market Bulletin: Cyber Risks and Exposures
[3] Federal Trade Commission v. Wyndham Worldwide Corp., et al., No. 14-3514 (3rd Cir. 2014) Appellant’s Opening Brief
[4] White Lodging releases information about data breach investigation at select food and beverage outlets