Does Your Hotel Have Cyber Liability Coverage?

As hotels continue to innovate with both guest-facing and back-of-house technology, they're also making themselves a more prominent target for cyber criminals. To help hotels prepare for the eventuality of a cyber attack, Samantha Ahuja, partner in the Hospitality and Commercial Real Estate Development & Finance practices, at Morris Manning & Martin, LLP and Molly Kacheris, associate in Morris, Martin & Manning, LLP's Commercial Real Estate Development and Finance and Hospitality practices, compiled a list of procedures hotels could follow.

In part one of this two-part article, they discussed how hotel owners and operators can limit the amount of unknown risk and liability with PCI-DSS compliance and by implementing other preventative measures. Here, in part two, they 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.

Contract Protections

Both parties to an agreement should carefully and expressly draft contract provisions to allocate the responsibilities, costs, and risks related to cyber security. Since this is still an evolving and growing area of the law, any contract provision should allow some flexibility for the potential for new federal and state legislation related to cyber security. The parties should also consider how the public relations aspect will be handled and who will bear the costs of those expenses.

Generally, a hotel operator only indemnifies the hotel owner for the operator's grossly negligent or willful acts. Therefore a typical indemnification provision would not cover a cyber security breach, absent gross negligence or willful misconduct of the operator. Hotel owners can seek to be indemnified specifically for a security breach of the operator's systems and the resulting loss or disclosure of confidential information. Hotel owners would request this indemnification cover all liability including third party claims, cost of investigation of a data breach, notification of customers and agencies, setting up call centers, public relations, legal costs, credit monitoring costs, and other costs to correct the breach event. Hotel operators would likely push back on any increase in their obligation under an indemnification provision.

In addition, hotel owners should set forth specific covenants on additional security requirements designed to prevent breaches. Hotel owners should require that the hotel manager covenants to ensure compliance with the minimum standards required by the cyber liability insurance policy. These covenants could also set out specific protection requirements that are more extensive than the minimum requirements set out by PCI Security Standards Council or the insurance requirements, such as notification to owner within a reasonable amount of time after a suspected or actual data breach.

Many hoteliers erroneously assume that if the breach is to or through their franchisor's reservation system that the franchisor will cover the franchisee in the event of a breach. Under may franchise agreements' indemnification provisions, the hotel owner will often be responsible for indemnifying and defending the franchisor from a claim of a data breach.

The parties should also establish which party is responsible for obtaining and maintain cyber liability coverage and the minimum policy limits.

Cyber Liability Coverage

Both hotel owners and operators have a need for cyber liability insurance and the parties should work together to avoid gaps in coverage. Most general liability policies do not cover cybercrimes or costs associated with a privacy event or breach. Some even specifically exclude losses incurred because of the internet or computer systems. A tailored cyber liability policy, on the other hand, typically provides first party protection and third party protection for events arising out of cybercrimes or data breaches.

The parties should also establish which party is responsible for obtaining and maintain cyber liability coverage and the minimum policy limits.

Cyber Liability Coverage

Both hotel owners and operators have a need for cyber liability insurance and the parties should work together to avoid gaps in coverage. Most general liability policies do not cover cybercrimes or costs associated with a privacy event or breach. Some even specifically exclude losses incurred because of the internet or computer systems. A tailored cyber liability policy, on the other hand, typically provides first party protection and third party protection for events arising out of cybercrimes or data breaches.

First party protection protects the policyholder's business from harms resulting from a privacy event or data breach. First party insurance also covers the cost associated with the privacy event including forensic study, public relations, regulatory compliance costs, notification costs, and even fines and penalties. Parties can also purchase foreign notification coverage or contingent business interruption coverage (including decreased in income due to poor public relations surrounding a data breach).

Third party coverage provides protection from suits from injured third parties. Lawsuits can arise from breach victims (individually or as a class action), issuing banks, the Payment Card Industry, and local and federal regulators.

Loss of digital asset coverage can be purchased to provide coverage if a software asset is damaged or destroyed. Insurance companies also offer coverage for cyber extortion or cyber terrorism, under which the insurance companies will pay off threats to protect the data systems.

Cyber liability insurance is a relatively new concept that is quickly growing in popularity. The ability to negotiate better terms and conditions is still available, but as cyber liability insurance becomes more mainstream the ability to customize may decrease.

Emerging technologies present additional hurdles to data security. Hoteliers should protect themselves from a privacy event or data breach on every level they can to limit the liability and bad public relation ramifications. They should start with prevention by maintaining PCI-DSS compliance and implementing other preventative measures. Hoteliers should then allocate the burden of potential liability and the obligations to maintain compliance standards to the appropriate party through carefully drafted contract provisions. Finally, hoteliers should purchase cyber liability coverage to protect themselves and the hotel from the legal ramifications and the public relations damages that result from a data breach.

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.