HOTEL BUSINESS REVIEW

DECEMBER FOCUS: Hotel Law

Not-So-Suite Cybersecurity Concerns in the Hospitality Industry

By Julia Kadish Associate, Sheppard, Mullin, Richter & Hampton | December 2023

This article was co-authored by Lauren Stewart, Associate, Sheppard, Mullin, Richter & Hampton LLP

Guests attempt to get into their hotel rooms with the room keycards, but the keycard system is not working.

The group of friends celebrating a birthday at the hotel bar goes to "cash out," for the night, but the register and credit card payment terminal are reading back an error code.

Potential guests are trying to make reservations through customer service in the city where the Super Bowl was just announced, but the phone lines are down. A bad actor is in the hotel lobby attempting to steal online credentials from guests through the hotel's Wi-Fi.

These are all very real threats that operators in the hotel industry face on a daily basis. Unfortunately, ransomware and other types of cyber-attacks are no longer atypical. When hotel guest data or technology supporting the hotel industry are compromised, links in the chain within the hospitality industry may be threatened.

Given these ever-increasing risks, businesses in the hospitality industry should stay vigilant in developing and maintaining a comprehensive cybersecurity program and procedures designed to secure and protect personal information. Below, we discuss what companies in this industry may want to consider from a legal perspective in their cybersecurity readiness efforts.

Know Your Data and Where it is At

Before an organization establishes and maintains a cybersecurity program, it helps to have a firm understanding of the type of information that it collects and where that information is stored. The hospitality industry sits in a peculiar position because of the opportunity for multi-modal interactions with guests and the surprisingly wider swath of information it may ultimately collect in the course of running its business.

Data collection could take place at every stage of a guest's stay at a hotel. If the guest books online, a guest's personal information and credit card information are provided, and that information often remains stored (in some form) when the guest arrives. Hotels typically require a guest to provide identification such as a driver's license or passport, and the hotel may store that information as well. Hotels may collect additional guest data in order to store guest preferences, to operate loyalty or reward programs, or to track guest feedback. Different

systems, vendors, and third-party tools or applications are used for each of these functions (and some functions themselves require multiple vendors).

Know Your Potential Attack Vectors

An organization's cybersecurity posture is only as strong as its weakest link. The hospitality industry probably knows this more than most. Hotels may employ individuals across a wider variety of roles and functions than a typical standalone company. Hotels often include businesses within the operation that open up additional points of risk, such as spas, restaurants, retail, and bars. With such a disaggregated workforce, hotels face increased points of entry for bad actors.

Hotels can mitigate this risk by requiring consistent data privacy compliance across all employees and tenants. Beyond privacy, a comprehensive and coordinated approach to privacy compliance can also help to ensure a consistent and exceptional guest experience. And while a lot of businesses may try to train their employees to understand the importance of customer data and how it may be processed, this can be a particularly challenging task for the hospitality industry.

Given the wide range of employee roles, the onboarding, training, processes and procedures, and type of skills needed for day-to-day operations varies greatly across the hospitality workforce.

From corporate employees to the front desk staff, to outsourced contractors and housekeeping, trying to ensure that such a broad workforce is trained on how to recognize and report social engineering attempts is no small feat. Organizations may want to consider each potential "entry" point for a cyber threat, identify what systems store guest and employee data, and think about how employees typically interface with these systems in the course of doing their job, and then craft tailored cybersecurity training exercises for each.

But, there are also other more creative ways in which bad actors may infiltrate systems and try to gain access to personal information. Thinking through all potential ways in which threat actors may infiltrate those data points is a separate, but worthwhile exercise. For instance, call center and IT support may have access to this personal information. With more sophisticated attacks occurring through the use of artificial intelligence – i.e., voice phishing to trick IT support or call centers into bypassing multi-factor authentication – vendor diligence of any third party support as well as ongoing audit and monitoring of these third parties can be helpful to companies.

Know What Laws May Apply

Adding to the complexity for hotel operators is the patchwork of potential data security laws that may apply. These laws may apply based on certain types of information that hotels collect, and/or because a company collects information from residents of the impacted state or territory. In the US, at least twenty-two (22) states have laws that require companies to protect personal information. Some of these state laws contemplate that specific requirements be addressed in a data security program (e.g., written information security policy, vendor contractual requirements, employee training, a designated person in charge, etc.). Others generally require that "reasonable security" measures be deployed.

Aside from US requirements, the hospitality industry should consider that guests may be residents of other countries, potentially triggering applicability of international privacy laws like the European Union and United Kingdom's General Data Protection Regulation (GDPR). Often, these international laws apply extraterritorially (i.e., to non-EU/UK based businesses) where a company offers services to or "monitors" the behavior of individuals in the EU/UK. While these more "comprehensive" international laws may not necessarily be more proscriptive than US requirements when it comes to specific data security measures that should be used, they carry weight of added enforcement oversight and potential fines.

In addition to statutory requirements, there are also industry and self-regulating standards with which hotels may need to comply. Hotels usually process a high volume of credit card transactions, which typically occur vis-a-via payment terminals (e.g., the front desk, parking garage, restaurant, etc.), by phone, or online (website or mobile app). The collection of payment card data triggers the Payment Card Industry Data Security Standard (PCI DSS) requirements. These robust standards could apply in addition to the myriad of other statutory requirements. Contractual requirements between business partners (as discussed further below) may also set forth expectations to comply with industry standards such as the National Institute of Standards and Technology (NIST) or to receive SOC 2 certification.

Aside from the specific measures that companies may be required to use to protect personal information, when a company faces a data security "breach," they face another patchwork of potential requirements. Every state in the US has enacted a data breach notification law – and some have multiple. There are a host of industry-specific laws that may require data breach notification. For hotel brands that are public companies, the SEC recently updated its data breach notification requirements imposing an exceedingly fast four business day notification period. This is one of the most aggressive turn-arounds in the US in terms of data breach notification requirements.

Under the new rule, a public company that suffers a "material cybersecurity incident" will have to file a Form 8-K disclosing the incident within four business days after the company's materiality determination. Material means it is substantially likely that an investor would consider impact of the incident important in making an investment decision, or if it alters the total mix of available information.

The hospitality industry was the first to test the waters of this new rule. Recently, MGM was the first to file an SEC Form 8-K under the SEC's new cybersecurity disclosure rule. Shortly thereafter, Caesar's also submitted a cybersecurity disclosure to the SEC. Both companies have been faced with a slew of class action lawsuits in the weeks following their initial disclosures.

Aside from state and federal requirements, contracts between business partners also typically set forth specific triggers for notification. Below, we further discuss how these agreements between different parties in the hotel ecosystem may help standardize and allocate responsibilities when it comes to data security.

Know How These Responsibilities are Shared

When developing a cybersecurity program, those within the hospitality industry should think about which party should be responsible for defining the requirements and which party will be responsible in the event something goes wrong. Depending on the structure of hotel management, many hotel developers elect to enter into either a franchise agreement or a hotel management agreement. A franchise agreement allows the hotel to operate under a hotel brand name, and acts as a license for the hotel operator to do so.

A hotel management agreement is an agreement between a hotel developer and a hotel manager to establish guidelines from the hotel owner that a hotel manager must follow. Both franchise agreements and hotel management agreements typically contain standards and requirements for the storage of personal data. These agreements may also include procedures for what to do in the event of a data breach, which may involve notifying the other party to the agreement, cooperating with investigations into the breach, and remediating the breach.

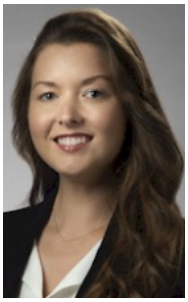
Some hotels may also lease space within their facilities to third party vendors to offer services like a spa or restaurant. These are typically evidenced by the hotel operator and the tenant entering into a lease. When negotiating a lease, a hotel operator is typically in the best position to establish how guest data may be collected and stored and to require that the tenant comply with all applicable data protection and privacy laws.

No matter what, hotels are subject to complying with local, state, and federal law with respect to collecting, using, and storing personal information of guests and employees. Franchise agreements, hotel management

agreements, and leases can give hotel operators a chance to contractually ensure that personal data is being stored consistently and that all parties are aligned on what to do in the event of a data breach. While cyber insurance can help mitigate the expenses arising out of cyber-attacks, companies should be mindful of the notification requirements under these policies and the growing list of possible exclusions to coverage.

Summing it Up

For the hospitality industry, cyber-attacks may not only pose significant legal risks, but PR and brand perception risks. While guests want to enjoy themselves and feel "secure" when staying at a property, they also want to know that the information they entrust to hotels is equally protected. Developing and maintaining data security compliance standards will help hotels to have a good understanding of the information they collect, the measures that should be used to protect it, mitigate the risk of legal exposure, and confirm that the standards and expectations for these data security measures are intended to be applied consistently across properties and owners.



Ms. Stewart

This article was co-authored by Lauren Stewart. Ms. Stewart is an associate in Sheppard Mullin's Chicago office and a member of the firm's Hospitality Team. She received her JD., cum laude, from the University of Illinois, and her B.A., cum laude, from Hope College. Ms. Stewart concentrates her practice on commercial and residential real estate development throughout the U.S., including construction and design contracts, lending and finance, and sales and acquisitions. With respect to property development, she has experience in drafting design, construction, project management and other consulting contracts. In the hospitality sector, she focuses on design and construction contracts, management agreements, and other operations contracts.

Ms. Kadish

Julia Kadish is an associate in Sheppard Mullin's Chicago office and a Lead Associate of the firm's Privacy and Cybersecurity Team. She is certified by the International Association of Privacy Professionals for CIPP/US, CIPM and CIPT. Ms. Kadish received her J.D., cum laude, from the University of Notre Dame, and her B.S. from Indiana University - Bloomington, with distinction, Honors Notation. She helps guide companies on how to lawfully collect, use, and share information. She reviews company products and services for privacy implications providing practical advice on legal requirements and specific operational advice for compliance. Ms. Kadish also works with clients on data security matters, advising on proactive measures such as policies, procedures, and incident response plans. She helps companies respond to data breaches from initial response and investigation to notification and ongoing support in state, federal, and international regulator inquiries.

Extended Biography & Contact Information

Share this article with your industry colleagues