Beazley | Beazley Breach Response Services

ECKERT SEAMANS
ATTORNEYS AT LAW

The Unique Challenges of Data Security for the Hotel Industry

Sandy B. Garfinkel, Eckert Seamans Cherin & Mellott, LLC

The hotel industry has been in the news frequently over the past year as a result of multiple and significant data security incidents. Nationally recognized hotel and resort brands continue to suffer by cyber attacks, including theft of payment card data from their retail or food and beverage outlets, and at times theft of guest data from reservations and management computer systems. In addition, less sophisticated data incidents regularly occur through theft or loss of mobile data and paper data.

Why are hotels such frequent targets? What makes them uniquely vulnerable to information threats? This article will examine those questions and suggest certain measures that hotel companies can employ to try to mitigate the risks to information that they own or possess.

Hotels face unusual problems when it comes to cyber security and vulnerability to data theft or loss because of traditional three-party ownership/management/franchise structures, as well as the way hotels tend to operate.

Multiple parties are involved in the equation

For branded hotels, typically at least three parties are involved in a functioning hotel business: the **franchisor or "brand,"** the **owner** (or owners' group) and the **operator** (or management company). Each of those entities plays a particular role in the function of the hotel as a business, and each may have its own computer systems or stored information:

Franchisor

- Owns the "flag" of the brand, and in exchange for use of its marks and marketing services, can impose its own standards for hotel features, including the process for booking rooms;
- Typically mandates that the owner install a particular hardware/software suite to handle the reservations functions;
- Maintains ownership and control of that system through contractual means; and
- Typically claims ownership of guest data that is input into the reservations system by hotel employees or others.

Owner

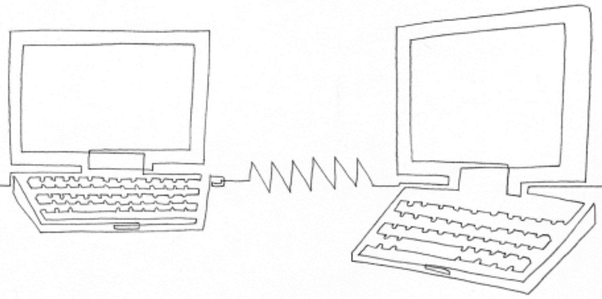
- Typically not the brand; could be individuals, investor groups or major asset holding companies, including investment funds, insurance companies, banks;
- May have varying degrees of involvement in operational issues that include guest or employee data; and
- May own separate "point of sale" payment card systems for food and beverage or retail outlets situated within the hotel

Operator

- If independent from the owner, will usually have a management agreement with the owner that establishes an agency relationship for purposes of all day-to-day hotel operations;
- Third-party operators are usually the formal employers of hotel personnel and maintain all employee data (including Social Security numbers); they are also responsible for employee information security training and the implementation of information security policies;
- May collect guest data before inputting it into the reservations and management system owned by the franchisor, if the hotel is branded; and
- May obtain and maintain payment card information associated with group bookings.

Sometimes the complex relationship between franchisors, owners, and operators requires that information be shared, or that separate computer systems be tied to each other. For example, as indicated above, major hotel brands require all of their franchised hotels to use the brand's reservations and management computer system when booking or checking in all guests. Thus, hotel owners and operators are forced to have their own on-site personnel use the computer system of another company when transacting business with guests. In addition, hotels, like other consumer businesses, often permit interfacing between their own computer systems and those of third-party vendors or credit card processors.

beazley



All of this means that hotel systems are to some extent dependent upon the security measures and practices of other entities which the hotels do not control. A classic example is the Wyndham Worldwide breaches which occurred 2008 and 2010, where hackers were able to penetrate Wyndham's central reservations database through a hack of a single franchised hotel, and then use the Wyndham system's connections to dozens of other individual franchised hotels to steal hundreds of thousands of sets of credit card data.

Hotels do business by payment card

Credit and debit card data has long been a preferred target of data thieves. Payment by card is the mainstay of most hotels, not only for guest bookings but for food, beverage, and retail transactions as well. Therefore, hotels represent a tantalizing treasure chest of data for cyber criminals to try to crack open.

The Wyndham breaches mentioned above, where the reservations system was the subject of the attacks, were certainly notorious in the world of hotel data incidents, but statistically most credit card data theft in hotels occurs due to malware affecting hotels' separate point-of-sale (POS) systems, rather than the brand reservations systems for guest room bookings. Of the fourteen most high-profile hotel company data breaches that have occurred since 2010, thirteen resulted from malware affecting POS systems in hotel restaurant and retail outlets.[1] Cyber criminals, through a variety of methods, are able to infect hotel POS systems with credit card data-scraping malware that captures personal account data at some point during the payment process.[2] This malware is often capable of moving between connected hotel systems and may infect groups of hotels that are either related by common brand or by a common third-party operator.

As discussed above, franchisors will commonly specify within franchise agreements that they are the owners of guest information that is entered into the reservations and management systems that they mandate for use at their franchised hotels. However, franchise agreements typically won't address the ownership of guest payment card data that is entered into separately maintained hotel POS systems at food and beverage outlets. The food and beverage POS systems are not commonly owned or controlled by franchisors.

Moreover, the management agreements between third party operators and hotel owners don't usually expressly address ownership of POS payment card data, either. This creates a certain degree of tension because operators are responsible for the day-to-day handling of protected data, and an operator's employees are the ones accessing and using the POS systems. The operator is also the party obliged to maintain compliance with Payment Card Industry Data Security Standards ("PCI-DSS") for the hotel's systems that receive or store payment card data. On the other hand, the hotel owner is typically the contracting party with the payment card processor that receives and processes the POS system card transaction entries, and the owner is therefore considered the "merchant" with contractual obligations to protect payment card data entered into the POS systems.
When a hotel POS system breach incident occurs, it is the standard industry practice that the hotel owner is regarded as the entity responsible for all legal response duties as the "owner" of the affected data. The operator may actually handle execution of the response obligations, but it almost always does so in its capacity as agent for the hotel owner, and costs of response -- including investigation, notification, fines and penalties – are commonly charged to the hotel owner.

Some hotel credit card compromises are not high-tech in nature. Many hotels still tend to receive faxed credit card authorization forms for company bookings or group bookings, and often the faxed paper forms, which contain credit card numbers and expiration dates, are kept in a non-secure manner, such as in binders behind the hotel front desk. These paper forms are susceptible to being lost or stolen, and while many state breach notification laws do not expressly cover loss or theft of paper data, a growing number of state laws do. For example, the data breach laws of California, Hawaii and Alaska all protect data in any form, including paper, that contains personally identifying information.

Employee turnover and fluidity contribute to security problems

In the hotel world there tends to be a high degree of movement of employees in and out of particular properties. Hotel operators will transfer their skilled employees to other locations where they may be needed. Employees in less skilled hotel jobs tend to come and go frequently as well. Owners may decide to change third-party operating companies, and the new operator will bring in its own management-level employees to manage the hotel. Maintaining a consistently trained workforce at hotels can be a challenge.

In recent years many information security industry experts have identified a company's employees as its most vulnerable point from a data security perspective.[3]
A fluid workforce means that it is more difficult to train employees in the secure receipt and treatment of personal information, in complying with privacy and security policies, in protecting and changing user access credentials, and in being alert for social engineering attempts. Keeping up with which employees have access to different levels of information is also challenging when there are frequent changes of personnel at particular job levels. Only certain job functions within a hotel setting

require access to guest or employee personally identifying information, and hotel companies (as well as companies in other industries) are not always as careful as they should be about controlling access by role (e.g., job grade or description) and making sure access is eliminated when an employee moves out of a particular position or is terminated.

How can hotel companies better prepare for and combat cyber threats?

While hotels have unique problems that tend to make them more vulnerable to threats of compromise and theft of personal information, hotel companies can prepare for and mitigate against such risks, and there are lessons to be learned from looking at hotel data incidents. From analyzing recent hotel breaches, the following practices could have mitigated or prevented such incidents.

Contractual risk-shifting and secure handling requirements

Franchisors, owners, and operators, in their dealings with each other and third parties such as vendors and contractors, can help to control the risks inherent in sharing systems or information with others. Requiring specific cyber incident indemnification, where negotiating leverage permits, is useful to protect hotel companies from the economic consequences of a breach incident caused by or contributed to by another party. In addition, contract provisions requiring compliance with minimum information security standards (e.g., compliance with PCI-DSS or mandating third-party compliance with a hotel company's own security policies) can reduce the risk of cyber incidents.

Employee policy enforcement and training

Despite the fluidity of management and staff employees that is attendant to operating a hotel, operators can and should consistently update their employee policies on data security and rigorously train employees who have access to data or systems. Where employees do not require access to personal information to perform their job functions, that access should be terminated. Policies concerning use of mobile devices, external information storage devices, and Internet usage should be enforced.

Guard guest and customer card data

Considering that POS malware attacks are the most common type of cyber incident affecting hotels, operators and owners should take extra care in selecting their POS system vendors and credit card processors. Agreements with those entities should be vetted and, if possible, modified to add protection and minimum data handling standards for the outside vendor. Compliance with PCI-DSS not only helps to ensure that data security software, hardware, and practices are safer but also helps to protect against fines and penalties which may be levied against hotels by the credit card industry for noncompliance with PCI-DSS when a breach occurs.
In addition, newer technologies are available which can increase security of credit card data. Examples include:

- End-to-end encryption (E2EE), also known as point-to-point encryption (P2PE): uninterrupted protection of payment data by encryption along the entire payment processing chain; when the data enters the payment system at a POS terminal it is immediately encrypted and remains that way until it reaches the processor or acquirer and is only then decrypted
- EMV or "Smart Chip" cards and readers: while EMV systems are increasingly common, as of the beginning of 2017 only approximately 44 percent of U.S. merchants had EMV-capable terminals, and only 29 percent actually have the software capable of reading the chip-based transactions.
- "Tokenization": a process of converting card data into unique, non-sensitive equivalents, known as "tokens," that retain the original data's essential information without compromising security.

Sandy Brian Garfinkel is the chair of the Data Security & Privacy Practice Group of the law firm of Eckert Seamans Cherin & Mellott, LLC. Sandy regularly assists the firm's business clients in all aspects of responding to data security incidents. He also counsels these clients in pre-incident planning and preparation. His primary focus in the world of data security is in the hotel industry, where he has worked as a commercial litigator for 20 years.
In addition to hotel companies, Sandy works with clients on data security and privacy matters across a variety of industries and sectors, including consumer products, insurance, education, health care, manufacturing and telecommunications.

[1] Timeline: The Growing Number of Hotel Data Breaches, Hotel News Now, June 17, 2016, http://www.hotelnewsnow.com/Articles/50937/Timeline-The-growing-number-of-hotel-data-breaches.

[2] POS Malware Families: An insight into the Behavior of POS Malware, AlienVault, Dec. 17, 2015, https://www.alienvault.com/blogs/labs-research/pos-malware-families-an-insight-into-the-behavior-of-pos-malware.

[3] *See, e.g.,* Richard Kam, The Biggest Threat to Data Security? Humans, of Course, The Privacy Advisor, Oct. 22, 2015, https://iapp.org/news/a/the-biggest-threat-to-data-security-humans-of-course/.

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.