SUMMARY PAPER

Hospitality Cyber Threats Are Alive & Well – Lessons From Recent Incidents

by Sandy B. Garfinkel, Esq.

The data incident involving the Starwood guest database was one of the most significant data security incidents in recent years. Publicly announced on November 30, 2018, the details revealed in the days and weeks following the announcement contain some striking reminders and new lessons for the hospitality industry. Here are some of the key facts of the incident:

- Marriott acquired Starwood in September of 2016, but Marriott continued to operate Starwood's guest database separately from Marriott's until a few weeks after the breach incident was announced.
- The unauthorized intrusion into Starwood's database occurred in 2014, but was not discovered by Starwood nor by Marriott later during the course of its acquisition of Starwood.
- The guest information compromised in the incident included name, address, phone number, email address, passport number, preferred guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preference, and in some instances, payment card numbers and expiration dates. It was ultimately reported by Marriott's forensic assessment provider the 383 million records were affected.

These facts underscore several crucial considerations for hotel companies regarding how guest data is collected, secured and retained. Some of these considerations aren't ones that our industry normally associates with data security concerns. Here are some of the key takeaways:

1. Data Security/Privacy is a Critical Due Diligence Consideration. In any merger or acquisition there are due diligence checklist items for the surviving entity. In the case of the Marriott/Starwood transaction the security breach of Starwood's database was not discovered prior to closing, but had it been, the implications for the deal could have been extremely significant. At the very least, action could have been taken to remediate the compromise at that time. In this day and age, cyber due diligence should be part of any merger or acquisition.

2. Retention of Large Amounts of Personal Information Carries Risk. Personal data is valuable for many reasons, but that value has to be balanced against the risk that accumulated

caches of personal data become rich targets for data thieves. For example, there were over 5 million unique unencrypted passport numbers and more than 20 million encrypted passport numbers that were compromised over the course of the Starwood data incident. The value to Starwood and Marriott of retaining that passport information is unclear, but the liability of replacing more than 25 million passports is enormous.

3. With GDPR and CCPA, the Definition of Protected Data Has Expanded. Before the effective date of the General Data Protection Regulation (GDPR) in May of 2018, most of the data involved in the Starwood incident would not have enjoyed any special protection. Under U.S. state law in most jurisdictions, even today, a person's name, address, phone number, and e-mail address are not considered Personally Identifiable Information or "PII." However, GDPR and the new California Consumer Privacy Act (CCPA) (effective January 1, 2020) have greatly expanded the scope of protected personal data to include virtually any item of information that can be used to identify an individual. A name, address, phone number or e-mail address are indisputably "personal data" under the GDPR.

4. Guest Reservation Systems Are Vulnerable On Both Ends. In branded hotels, franchise agreements always require that the hotels utilize the brand's reservation and management system, including brand-mandated hardware, software, portals and connections. This arrangement gives data thieves multiple targets from which to select when seeking to steal guest information. The Wyndham data incident of 2008/2010 was the first notable attack on a brand's central guest information database. While most hotel guest information data incidents in the past decade have occurred at individual hotels or discrete groups of properties, the Starwood incident proves that a brand's guest information database is still vulnerable.

2018 also saw a rash of low-tech social engineering attacks against individual hotels, and this type of attack has continued into 2019. Criminals commence these attacks by posing as brand systems support personnel and making phone calls to hotel employees. The employees are asked to provide their login credentials for the reservation management system.

***Cybercriminal**: Hello, I'm calling from [brand] system support. We're having difficulty with the reservation process on your end, and we need to check it. Can you please log in for me?*

***Employee**: Sure. [Logs in]*

Cybercriminal*: We're still having an issue. Can you please give me your username and password so I can try it on our end.*

Employee*: No problem. My username is … and my password is …*

Using the stolen credentials, the criminal remotely accesses the reservation management system and retrieved information about recent guest bookings, including guest names, addresses, phone numbers, reservation dates, and partial payment card information. Although the systems typically show only partial credit card number, in some cases the criminals are able to unmask the obscured numbers.

The criminal then calls guests with future reservations:

Cybercriminal*: Hello, I'm calling from [hotel name] regarding your reservation from [check-in date] to [check-out date]. We're having a problem processing your credit card. The last four numbers are [XXXX]. Could you please provide me with your full credit card information, including security code, so we can get that taken care of.*

Because the criminal has accurate information about the reservation, the guest is more likely to fall for the scam. Once the guest has supplied the card information, the criminal quickly racks up fraudulent charges. Fortunately, most guests don't trust these calls, but they are bad for the reputation of the hotel and brand. Depending on what information is exposed, the unauthorized access to the reservation management system may legally be considered a data breach that requires notification to affected individuals and regulators.

To help protect your organization from these types of social engineering attacks:

- Change employee passwords at frequent intervals.
- Alert employees to this type of attack and train them in how to respond.
- If possible, implement multi-factor authentication for any access to the reservation management system.
- Audit which employees have access to the reservation management system and disable access for employees who have no business need for it, including employees who have been terminated or who have changed roles.
- Protect partial payment card information so obscured numbers can't be unmasked.