OWNER'S MANUAL

THE BUSINESS OF HOSPITALITY

SMART STRATEGY

Data Security Soft Spots

SAFEGUARDING A PROPERTY AGAINST CYBER ATTACKS

BY SANDY BRIAN GARFINKEL AND GOSIA KOSTUREK

THE HOSPITALITY 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 such as IHG, Sheraton Hotels & Resorts, Hyatt Corporation, Hilton Worldwide, and Trump International have been the target of recent cyber attacks

According to Mark Voortman, Ph.D., head of the information technology program at the Pittsburgh-based Point Park University's Rowland School of Business, "International or U.S.-based hotels can be attractive to hackers because of the disruption, embarrassment involved, but mostly for monetary gain." He points to a recent example of hackers compromising an Austrian hotel's computer system so that hotel doors were locked, leaving guests stranded in the lobby. "Cyber attacks can come and go but defenses have to be ready at all times," he adds.

So what attracts data thieves to hotels? And how can hoteliers mitigate the risks? The answer is by looking at key vulnerabilities.

Credit and debit card data is a preferred target of data thieves, and these thefts occur in hotels when cyber criminals infect point-of-sale (POS) systems or property management systems (PMS) with malware that captures personal account data. Malware can move between systems to infect groups of hotels related by brand or third-party operator and may operate for several months or even years before being detected. In February, it was reported that of the 21 most high-profile →

hotel company data breaches that have occurred since 2010, 20 of them were a result of malware affecting POS systems in hotel restaurant, bar, and retail outlets. Paper forms can also be compromised, and while many state breach notification laws do not expressly cover loss or theft of paper data, a growing number of state laws do. Identity thieves have also targeted guests unfamiliar with the area or hotel with schemes like posing as being from the front desk and asking for updated credit card information.

Hotel 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 the Payment Card Industry Data Security Standard (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 when a breach occurs.

In recent years, many information security experts have identified a company's employees as its most vulnerable point from a data security perspective. Because hospitality employees frequently move in and out of particular locations, maintaining a consistently trained workforce is a challenge. In a fluid workforce, it is more difficult to train employees in secure handling of personal information, complying with privacy and security policies, and protecting and changing user access credentials. →

CONNECT *the* DOTS Fast Response

CHRIS ZOLADZ founded Navigate LCC, an information protection privacy consultancy, eight years ago to help clients create and refine data breach response plans. According to Zoladz, when a hotel is victim to a cyber attack, it can take anywhere from days to months to determine what actually happened. Therefore, once an attack is confirmed, hotels must act quickly. Zoladz offers four tips for hoteliers facing fallout from a data breach.

1. **Don't deny the problem.** "First and foremost, hoteliers must fight the urge to deny that something bad has happened. Regardless of the nature of the attack, when hoteliers deny the presence of a problem, they are losing valuable time."

2. **Act fast.** "The first 24-48 hours are really critical to minimize damage, preserve the brand's reputation, and maintain customer trust. Timing is everything in a breach response. You must be able to quickly identify the problem to limit losses."

3. **Engage your staff.** "It is so important to engage all of your team members when it comes to a breach response. While it's always better to have a plan, if you don't, then you should immediately identify and engage the necessary members of your team. A timely response is generally going to include representatives from the legal department, information technology, security, communications or public relations, and human resources. You must bring everyone together quickly to control the damage and ensure everyone is on the same page."

4. **Identify a team leader.** "Who is the quarterback of the response? Who is going to ensure that all tasks are completed to comprise an efficient response? Who is going to establish the roles and responsibilities of the various team members? Who is going to approve press releases or responses to the media? Some of that may already be in place during a normal business day, but when these events happen, it is no longer a typical day."

EXPLAINER

PCI-DSS

"PCI-DSS" REFERS TO THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS, WHICH IS A SET OF SECURITY STANDARDS DEVELOPED BY THE MAJOR CREDIT CARD COMPANIES. EVERY MERCHANT THAT TAKES CREDIT CARDS IS SUBJECT TO PCI-DSS THROUGH THE AGREEMENT IT HAS WITH ITS CREDIT CARD PROCESSOR. UNDER SUCH PROCESSING AGREEMENTS, THE MERCHANT AGREES TO COMPLY WITH PCI-DSS AND ACKNOWLEDGES THAT THE PROCESSOR MAY CONDUCT AUDITS TO ASSESS COMPLIANCE (SUCH AUDIT REQUESTS ARE OFTEN TRIGGERED BY A DATA BREACH). NON-COMPLIANCE MAY RESULT IN FINES OR ULTIMATELY IN THE REVOKING OF THE MERCHANT'S ABILITY TO TAKE CREDIT CARDS FOR PAYMENT.

Controlling employee access to different levels of information is made exponentially more challenging when there are frequent personnel changes. Only certain job functions within a hotel setting require access to guests' or employees' identifying information and companies must be careful to control access by job grade/description, as well as to eliminate access when an employee vacates a position.

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. In addition, to protect against identity thieves, employees should be trained on how to advise guests on potential risks, how to identify suspicious behavior, and when to report suspected identity theft or data breaches.

Operators can and should consistently update their employee policies on data security and rigorously train employees who have access to data or systems.

For branded hotels there are typically at least three parties involved in a functioning business: the franchisor or brand, the owner, and the operator. Each entity plays a particular role in the function of the hotel as a business, and each may have its own computer systems or stored information. The complex relationship between franchisors, owners, and operators sometimes requires sharing information, or connecting separate computer systems. In addition, hotels often permit interfacing between their own computer systems and those of third-party vendors or credit card processors. Therefore, hotel systems are to some extent dependent upon the security measures and practices of entities beyond their control. A classic example of this is the Wyndham Worldwide breaches that occurred in 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.

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 such as the PCI-DSS or mandating third-party compliance with a hotel company's own security policies can reduce the risk of cyber incidents.

In almost any industry, it's not a matter of how, but when data theft, cyber attacks, or accidental loss of data will occur. With a few key safeguards in place, your hotel can be well-positioned to not only rebound, but build trust and goodwill for the future.

- *Sandy Garfinkel is a member with the law firm of Eckert Seamans Cherin & Mellott, LLC. He is the founder and chair of the firm's Data Security & Privacy Practice Group and a member of its Hospitality & Gaming Practice Group. He can be reached at (412) 566-6868 or at sgarfinkel@eckertseamans.com.*

- *Gosia Kosturek focuses her practice on hospitality law and general corporate law at Eckert Seamans Cherin & Mellott, LLC. She is a member of the firm's Data Security & Privacy Practice Group and its Hospitality & Gaming Practice Group. Ms. Kosturek can be reached at (412) 566-6180 or at gkosturek@eckertseamans.com.*

Here are all of the products that can do the following:

KILL BED BUGS, DISINFECT, KILL MOLD, KILL MITES, KILL BACTERIA, DEODORIZE, KILL MILDEW, KILL FLEAS, SANITIZE, EFFECTIVE AGAINST MOST GRAM NEGATIVE AND GRAM POSITIVE BACTERIA, KILL ROACHES, KILL VIRUSES, ETC, ETC

STERI-FAB®

STERI-FAB®

MUCH MORE THAN A DISINFECTANT

800 359-4913 • STERIFAB.COM