Charlotte Baker, CEO, Digital Hands

New Security Threats Require Ongoing Diligence

Managed Security Firm Offers Best Practices for Hotels in Combating Growing Threat to Network Security

AS HOTELS EXPAND THE FUNCTIONALITY OF THEIR NETWORKS TO IMPROVE THE GUEST experience, they are presented with increased security challenges. These challenges span regulatory changes, new technologies and changes in operational processes. Managing the security component of these changes is complex, time consuming and requires a specialized skillset. Most hotel franchisees do not have personnel with these skillsets on staff. This means that third-party specialists must be engaged, either through their brand, by the hotel operator or both. In this executive Q&A, *Hospitality Technology* talks to Charlotte Baker, CEO of Digital Hands — a global provider of managed security services with headquarters in Tampa., Fla. — about some of the latest challenges hotels face in protecting their networks, their guests, and their businesses.

HT: We continually hear that the hospitality industry is a common target for hackers. Can you provide some context to the volume and type of threats that these and other industries face?

CB: In just the past three years, the threat landscape has increased exponentially. There are 55,000 new pieces of malware each day, and that's growing at a rate of 15% quarter-over-quarter. Approximately 75% of breaches compromised payment data and almost fifty percent of those gained access to user login credentials. The risk is made greater by the amount of time it can take to discover a breach — statistics show that almost 90% of data breaches go undetected for three or more weeks. As we know, the impact of something like is exponential, and includes not only the financial penalties and remediation costs, but also the loss of customer trust which ultimately means lost revenue.

Looking closer at the hospitality space, the accommodation and food service industry made up almost half of all breaches, and most attacks on hotel/retailers were done by organized criminal groups — 78% from Eastern Europe alone. The fact is, most hotel/retail attacks don't involve internal staff.

HT: How would you coach a firm to identify and manage its security needs?

CB: Currently PCI DSS is the primary security standard for hotels, though there are other standards including those set by card brands and other privacy laws, etc. The appropriate PCI DSS Self-Assessment Questionnaire (SAQ) is a good guideline to start to understand the complexity of your security requirements.

Beyond that, a merchant must begin with identifying the various regulatory, brand policies, privacy law requirements and the physical and electronic location of sensitive information. This information can include, but is not limited to, credit card data, customer information and employee records.

After you have identified your requirements, you must then triage the solutions, based on risk and exposure, while managing the expense. Meaning, you should "get the best bang for your buck". For example, restrict physical access to systems that have access to guest information. Make sure that only employees have access to computers that can access credit card, guest or employee information.

HT: Are these requirements only for digital data?

CB: No, this includes all types of data, physical and electronic. In the case of hotels, for example, access to guest data, whether printed or electronic, must be restricted to only those employees that need that data as part of their job requirements. This includes printed registration cards, printed folios and other guest data as well as access to the property management system. Access to employee data must be controlled in a similar fashion.

HT: Is a hotel responsible for their guests' mobile devices — such as a laptop or tablet — while they access the Internet?

CB: Any device that utilizes the resources provided by the hotel can lead to liability for the hotel. If a guest computer has access to systems that can access customer or employee data, a greater potential risk is present. Computing and mobile devices that use the hotel's guest network present a different set of lower-risk challenges.

HT: What are some basic security best practices a hotel should follow, and how can Digital Hands help?

CB: We recommend that merchants use firewall and intrusion prevention solutions, and isolate customer information from non-operational systems. Also, consider restricting physical access to systems that contain sensitive information based on job requirements. Time is truly of the essence during a cyber-attack, and proficiency in using security tools can mean the difference between thwarting an attack and assessing damage. The Digital Hands team of security experts brings a high level of proficiency to these challenging tasks using the customer's existing infrastructure or deploying industry-leading solutions. We provide customized services to meet our clients' needs, lettings you focus on your core business. HT

digitalhands
Digital Hands
www.digitalhands.com
sales@digitalhands.com
(855) 511-5114