DATA INSECURITY

AS HACKER ATTACKS INCREASE, HOTELIERS MUST TOKENIZE AND GO BEYOND PCI COMPLIANCE.

by **ADAM KIRBY, CONTRIBUTING EDITOR**

People often think of data security as protecting financial information, and while that is certainly a primary consideration, the concern should be much broader.

Many states and countries ascribe personally identifiable information — known to the security community as PII — with legal protection comparable to that of credit card data. What constitutes PII is almost limitless, from home addresses and emails to seemingly innocuous information like a person's favorite sports team or what spa treatments she has purchased; the muddled definition of exactly what PII encompasses is part of what makes protecting personal data such a complicated task.

"The challenge for hotels is that they really like information," says Bob Braun, a Los Angeles attorney who specializes in information security law for the hospitality industry. "They're collecting all kinds of information — home address, birthday, workplace information — that is very, very valuable to certain individuals who shouldn't be able to get it."

As hoteliers continue to expand niche marketing efforts and customer relationship management initiatives, they make their caches of PII data that much more attractive to criminals. Charles Carrington, a Deloitte & Touche information security consultant focused on the hospitality sector, says hoteliers need to look more skeptically at their hotels' PII collection practices. "Hotels are treating it as a compliance issue, rather than standing back and saying, 'What is the risk of gathering all this data?'" Carrington says.

Hoteliers need not abandon CRM

altogether, but they should have a defined plan for the personal information they do collect — specifically what it will be used for, what individuals in the organization have legitimate need to access it and how it will be safely disposed of when the time comes. “If it’s not needed, don’t collect it,” Carrington says. “You can’t lose what hasn’t been collected.”

Hackers target hotels

Hotels face outsized challenges in securely completing credit card transactions compared to other sectors. Retail and restaurants need only transmit sensitive data once per transaction, but hotels must send the same data at least twice, at the time of check-in and again at checkout, doubling the exposure risk. Moreover, while retail and restaurants might hold that data for a period past the transaction, the dispute window in those industries is usually about 45 days. Hotels may have to hold the data for six months or more after factoring in the advance booking window and a lengthier dispute period.

Hackers perceive that a successful data breach for hotels would be more lucrative than in other consumer segments, says Jeffrey Parker, vice president of technology for Stout Street Hospitality, a Denver-based management company. “Hotels have a big struggle — our average transactions are huge compared to retail or even restaurant transactions,” Parker says.

Indeed, the recent data breach of U.S. hotels managed by White Lodging Services Corp. — which exposed the names printed on customers’ credit and debit cards, credit and debit card numbers, the security code and card expiration dates — is a testament to how attractive the hotel industry is to hackers.

To mitigate this, look for tokenization to gain more traction in 2014 as a strategy to fend off card data theft. With tokenization, credit card data is replaced by what is essentially indecipherable coding before it is transmitted and later translated, so if the transmission were to be intercepted by hackers, the data would be worthless.

Even with tokenization, though, employee naiveté remains another hurdle to data security. Hospitality workers tend to want to help guests any chance they get, posing a data security risk through “social engineering.” A rudimentary example of this might be someone engaging a worker in friendly banter in an effort to procure a network access code. Or, more surreptitiously, a guest could offer a sob story about needing to urgently print a document and convince a front desk agent to insert a USB drive into a back-of-house computer, unknowingly uploading any number of malicious programs. Addressing social engineering challenges starts with retraining employees to maintain an appropriate vigilance about computer threats, says Stan Stahl, president of Los Angeles-based data security firm Citadel Information Group.

Beyond PCI compliance

Top executives need to be made fully aware of data security risks and continuously engaged in risk management. “This is not something that should be delegated to a compliance department, because the reputation of the organization could be in peril,” Carrington says.

Perhaps the most egregious data security mistake some hotel companies continue to make is failing to physically segregate guest Internet from back-of-house networks. In addition, the hotel’s credit card processing network should be physically segregated from all other networks.

Likewise, Stahl suggests designating a segregated back-office computer solely for online banking. “There’s no reason for a hotel not to be doing that, and yet I don’t know any that are,” he says.

If data must be transferred between networks, do so only on a secure network that can be tracked and logged.

DATA SECURITY TIPS

- Make sure computer programs are updated with the latest security patches. Daily updating is best, but weekly is the minimum frequency.
- Change passwords often.
- Control Internet access by installing site-scanning software that prevents employees from accessing dangerous websites, intentionally or accidentally. Similarly, control what can be downloaded onto hotel networks by blocking access to cloud storage servers like Dropbox and Google Drive, which can be used as attack vectors.
- Never allow a foreign USB drive on a back-of-house network.
- Issue policies governing explicitly what guest information franchisees and management companies are and are not permitted to collect.
- Consider buying cyber crime insurance; while banks typically reimburse individuals who are victims of fraud, businesses usually must absorb monetary losses. For a small company, a breach could be financially devastating.
- Create a detailed crisis management and brand protection plan if a breach does occur.

GRADUALLY TURNING

COST AND LINGERING SKEPTICISM ARE SLOWING NEW LOCK TECHNOLOGIES' UPTAKE.

contributed by CURTIS ANDERSON

Next-generation guestroom lock systems are slowly gaining steam across upscale and luxury segments as new-build projects and major renovations are being accompanied by RFID and NFC lock installations. Dedicated retrofit projects remain relatively scarce, though.

While reliable figures on locking-technology adoption are difficult to come by, it is clear RFID (radio-frequency identification) and NFC (near field communication, a communications protocol that allows devices to send and receive data instantly and securely over short distances) have not yet gained the hotel ubiquity that was being predicted a decade ago. That is due partly to the banking crisis of 2008 that scuttled many development and remodel plans.

In that context, the move to RFID and NFC is progressing about as rapidly as could be expected, says Jeremy Rock, president of Anaheim, California-based hospitality technology consultancy RockIT Group. "The installation of door locks is usually tied to new development and refurbishment projects, and unless there is a pressing issue with the locks they are rarely replaced as part of a technology refresh," Rock says.

Some hotel companies are making new lock technologies their brand standard for new projects. Hilton Worldwide is among the major brands requiring all new hotels and renovation projects that include lock replacement use RFID technology. Likewise, a pair of Bangkok-based companies, Onyx Hospitality Group and Minor Hotel Group, are both mandating RFID in their new-build properties. "We looked at our future technology strategy and decided that if we invest into magnetic stripe at this time we'll be investing into yesterday's technology, and with limited options," says Mike Stokman, director of information technology for Minor, which owns the Anantara Hotels, Resorts & Spas brand.

For resort operators with multiple points of sale and integrated vendors, like Destination Hotels & Resorts, Englewood, Colorado, RFID keycards can serve double duty for purchase transactions. That they need not even be keycards at all is an added bonus. "Wristbands, key fobs, cell phones and others offer interfaces with guest services," says Mike Shutts, vice president of corporate engineering for Destination. "Magstripe locks do not embrace vendor interfacing well."

Meanwhile, as NFC increasingly becomes an integrated part of consumers' daily lifestyles, most hospitality technology experts believe NFC will eventually become the default access format for hotels across segments and regions. At that point, guests will be able to use mobile devices to unlock their guestroom doors immediately upon arrival, without even needing to conduct a front-desk check-in process.

A key selling point for both RFID and NFC locks are their reliability; magnetic stripe cards can become deactivated when they come into contact with mobile phones, while RFID locks generally require less maintenance. These technologies also have a lower rate of misreads, which can be a point of maddening consternation for guests using magnetic stripe locks.

Aesthetic enhancements are a corollary benefit to NFC locks, along with RFID to a slightly lesser extent. Since these systems need not require physical contact between the "key" and the lock, visible locking hardware components will become obsolete, streamlining the appearance of hotel corridors.

Geoffrey Fordham, vice president of projects and product development for Onyx, says the sleekness of RFID and NFC plays a role in selecting locking systems for the company's new luxury brand, Saffron. However, appearance is subsidiary to brand reputation, system integration, maintenance, sales support and pricing. "The aesthetic will be an important factor as the door appearance will have to be carefully integrated with the corridor designs; however, the aforementioned points will have to be met first," Fordham says. "There are new designs on the market that allow the door lock to be fully integrated, basically hidden in the door, so it looks beautiful."

In general, though, the traveling public seems rather indifferent about advances in locking technology. Hoteliers see other capital improvements to technology, like faster Wi-Fi or bigger televisions, as being greater drivers of rate than locking systems. "I don't think that the majority of guests know the differences between the locks and technology," Rock says. "They primarily look at the aesthetics of the door lock and whether it's RFID or magnetic stripe."

Stokman, however, says the RFID locks in use at some Anantara properties still evoke a "wow" factor with guests.

Potential roadblocks

Critical-mass issues aside, some practical obstacles stand in the way of widespread RFID and NFC adoption.

The most obvious objection for hoteliers in adopting new locking systems is cost. A retrofit can cost US$300 or more per door, and RFID cards are more expensive than magnetic stripe cards, about US$1 on average compared to US$0.10. On the other hand, RFID keycards can be reused many times, assuming they are not lost or thrown away, whereas magnetic stripe cards lose their integrity in fairly short order. Then there is the issue of a guestroom with multiple occupants for a room; if the access device is a smartphone, then multiple devices will need to be activated.

Finally, the security of the lock systems is its own concern. Although it involved the older magnetic stripe technology, the 2012 hacking scandal involving Onity magnetic stripe guestroom locks has made hotel companies leery of vendors' claims that the newer systems are impenetrable to data theft and access manipulation.

"Until they prove that technology is 100% secure, or there is assurance from the manufacturers that they will compensate the owners and operators if a breach occurs, then it will continue to be slow adoption," says Tom McElroy, director of safety and security for Red Roof Inn, Columbus, Ohio.

"THERE ARE NEW DESIGNS ON THE MARKET THAT ALLOW THE DOOR LOCK TO BE FULLY INTEGRATED, BASICALLY HIDDEN IN THE DOOR, SO IT LOOKS BEAUTIFUL."

– GEOFFREY FORDHAM, VICE PRESIDENT OF PROJECTS AND PRODUCT DEVELOPMENT, ONYX HOSPITALITY GROUP