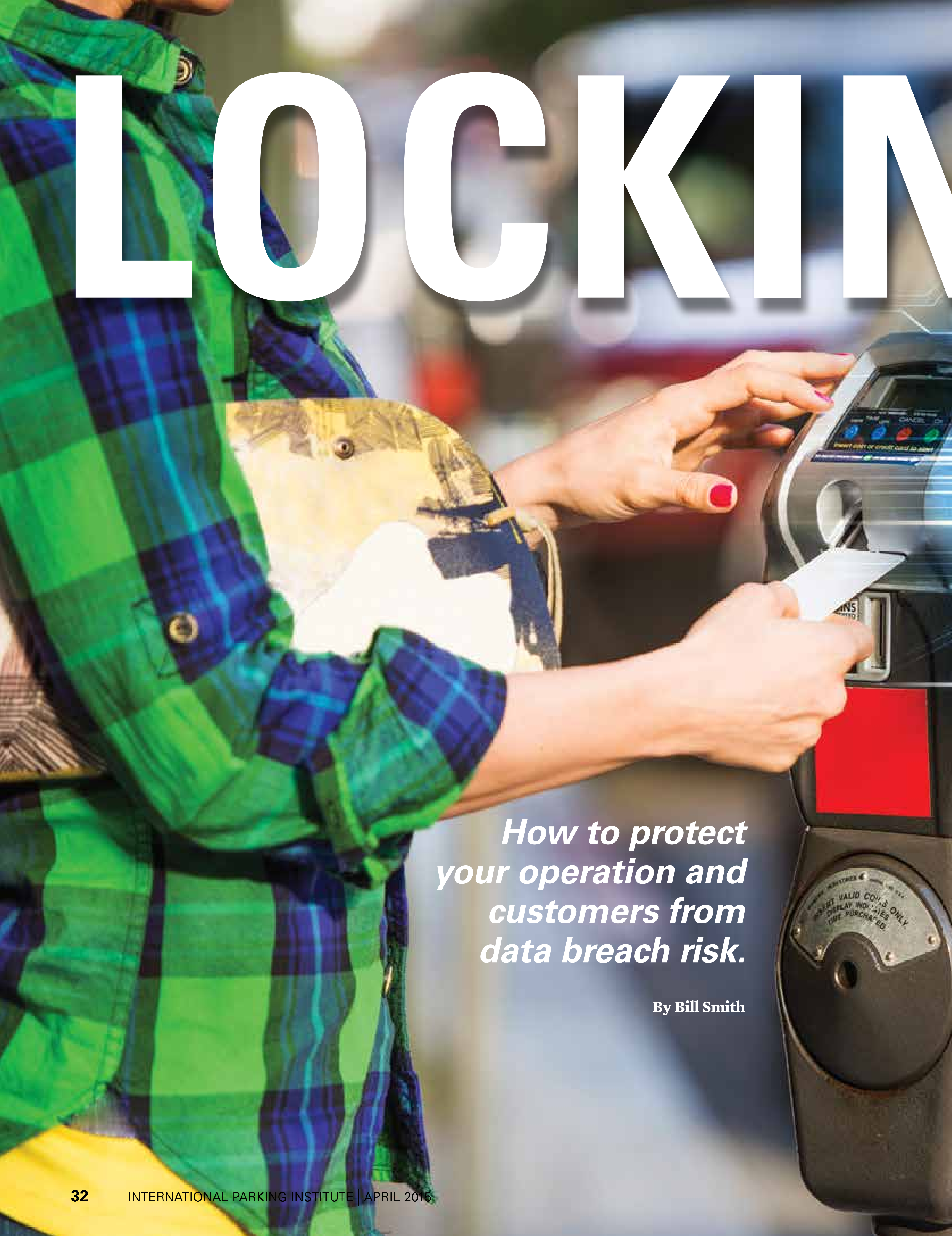
LOCKIN



How to protect your operation and customers from data breach risk.

By Bill Smith

NG DOWN

During the past decade, data breaches have become increasingly common. Retail and healthcare leaders such as Home Depot, Target, TJX, and Anthem, Inc., have been the targets of sophisticated attacks through which millions of customers' information was compromised. In this electronic age when our personal and financial data is often stored online, data security will continue to be one of the most challenging issues facing organizations that collect payments or personal data and store or transmit it online.

Unfortunately, the data breach trend has reached the parking industry. In the past year, several parking companies have experienced breaches. And while their effects were limited—certainly nothing close to the extent of the previously mentioned breaches—they illustrate the vulnerable position in which parking organizations find themselves.

"Everyone who accepts credit cards is at risk," says Patrick Brooke, director of technical services at Sentry Control Systems.

Brian McGann, parking consultant and data security expert with Walker Parking Consultants, says parking operators are particularly vulnerable today.

"There are bad guys out there who are always looking for new targets," he says. "Now that they have found some soft systems in the parking industry, they will continue to look for new targets in the industry."

Ensuring Compliance

Both Brooke and McGann say the key to ensuring that a parking system's operations are secure is to make sure that they are PCI compliant. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. The PCI DSS is administered and managed by the PCI SSC, an independent body that was created by the major payment card brands Visa, MasterCard, American Express, Discover, and JCB. Before purchasing a credit card processing system, operators should visit pcisecuritystandards.org to ensure the software they are considering has recently been audited and is PCI PA-DSS compliant.

Of course, not all threats come from outsiders. Employees, ex-employees, service personnel, and contractors can all turn out to be threats. That's why it's vital to ensure that security packages are set up to give the least amount of privilege necessary to perform a given job and to remove access as soon as it is no longer required.

McGann cautions that as important as PCI compliance is, it's not always enough.

"Owners buy systems that get audited out of the box, but that doesn't mean that the software will be secure in their own systems," he says. "Security is difficult and takes a lot of work, and owners and operators need to do their background work. There can be many holes, and owners and operators need to constantly be upgrading their systems and keeping up with new standards to keep ahead of the bad guys."

McGann stresses that most organizations should have a digital security expert, either in-house or as a consultant. That expert should understand the risks and tools available to protect against those risks, and he or she should know how to implement penetration tests to ensure the system remains invulnerable to attacks.

"This type of protection can be costly, but the cost of a breach is much higher," McGann says. "Lawsuits and fines arising from inadequate security can cost millions, not to mention the public relations costs and loss of trust among customers."

Brooke agrees that achieving 100 percent PCI compliance can be expensive and even cost-prohibitive for smaller parking owners. To offset the cost, he recommends relying on technology providers who offer assistance in meeting PCI compliance, including offering application and operating system security updates and patches and instant notifications when malware or threats are detected.

Big Companies, Big Breaches

Some of the largest breaches to happen during the last year hit big companies many of us thought had the resources to be immune—proving, of course, that no one is really safe when it comes to data security. According to *Forbes*, some of the biggest breaches of 2014 were:

- Neiman Marcus, where hackers used malicious software to steal the credit and debit card data of about 350,000 customers.
- Sally Beauty, which saw the theft of card data belonging to more than 280,000 customers.
- Michaels. Up to 3 million cards may have been compromised when the arts and crafts chain was hit in two different incidents.
- Affinity Gaming, which operates 11 casinos in the U.S., reported a data breach when its card processing system was infected with malware.
- P.F. Chang's China Bistro reported a breach that affected 33 restaurants in 16 states, including card numbers, cardholder names, and expiration dates.
- Albertson's and Super Valu, where a huge hack affected about 928 stores; the chains share technology to process payments.
- Community Health Systems, where information on 4.5 million payments was stolen in a cyber attack from China. This included patient names, birth dates, addresses, and Social Security numbers.
- Dairy Queen, where malware breached the data of almost 600,000 credit and debit cards from 395 stores.
- Goodwill, which was hit with a breach that took the data from 868,000 credit and debit cards in 330 stores.

He also advises owners and operators not to assume that a security system is secure just because it is new.

"I met an operator a few months ago who had recently installed a system and assumed his data was secure," he says. "However, when we checked, we found that the software he had installed wasn't Payment Application Data Security Standard (PA-DSS) validated. He learned the hard way that not all new out-of-the-box solutions are up to the job."

Tokenization and End-To-End Encryption

According to David Leppek, president of Transaction Services, a transaction management company based in Omaha, Neb., much of the security problem facing the parking industry revolves around how operators are handling data. He says that rather than storing credit card data, operators should rely on tokenization to record customer data.

A token is a complex alphanumeric number that's tied to a customer and his or her payment type. The token has no meaning or value on its own, but rather is merely an identifier that is tied to an individual customer.

"Tokenization is an added level of security against the types of backdoor data breaches that have hit the parking industry," he says. "If a criminal exploits a back door to try to steal data, all he'll find is a token. There's nothing valuable to steal."

Leppek does offer one word of caution to owners, though: Make sure you aren't held hostage by the token. Owners should be able to move their tokens from provider to provider if they find a better security package in the future.

"Tokenization offers a level of security that's rare in the parking industry," he says. "There are still owners who keep credit card numbers in shoe boxes and Rolodexes!"

Encryption is another security element that's vital to parking owners and operators. Improper encryption can undermine security and inadvertently leave parking owners and operators at risk.

"There are some solutions that have the provider take credit card data and transmit it to the security provider to be tokenized," Leppek says. "If that data isn't immediately encrypted before being submitted for tokenization, it can be intercepted when it is being transmitted."

Leppek advises that every credit card's data be encrypted the moment it is swiped. Further, he recommends that advanced encryption standards with 256 bit encryption be used, and that the data be transmitted over a 256 bit SSL tunnel.

Back to Cash

The spate of data breaches in recent years has many people concerned about the well-being of their data—understandably so—and more willing to use cash to pay for parking. According to Bryan Alexander, Crane Payment Innovations, while cash has always been a popular way to pay for parking, recent breaches have further increased old-fashioned money's prominence.

"People are more mindful of where they are using credit cards, and they are more likely to use cash," Alexander says. "When parkers have the option of paying with cash, they can just pay and walk away without worrying about whether their personal and financial data is at risk."

"Parking owners and operators came to rely more on credit card payment because the transactions were quicker and reduced the risk of theft," he continues. "However, today's cash payment equipment has improved by leaps and bounds, permitting extremely fast transactions and allowing parkers to pay and be on their way in just a matter of seconds.

"Cash payment is also incredibly secure and efficient today," Alexander explains. "Modern machines come equipped with two to four recycling modules, eliminating the cost of having staff visit machines daily to retrieve the cash. And because all modules are always locked and monitored by internal sensors, no one is able to touch the cash until it arrives in the counting room. This eliminates the risk of theft."

Adaptability

Of course, whether a facility is accepting cash, credit, or both, every system needs to have the capability to adapt as new threats appear and new security tools are introduced to fight them. Adaptability will be particularly important in the coming months for American owners and operators as the U.S. moves to the Europay, MasterCard, Visa (EMV) credit card standard (see the March issue for more). EMV, which has been the European standard for credit card technology for more than a decade, revolves around integrated circuit cards rather than magnetic stripes to authenticate credit and debit card transactions.

Soon, U.S. consumers will use credit cards with chips inside them. The chips provide more secure authentication to protect consumers' data. Like all retailers and service providers that accept credit cards, parking facilities need to be able to accept EMV payments by October 2015 or risk facing liability if a fraudulent transaction takes place.

The credit breach trend that has bedeviled the retail world for years has finally come to the parking industry. It's a challenge that must be met by parking owners and operators, and it's not going away anytime soon. However, by turning to standards that meet PCI requirements, owners and operators can dramatically reduce the risk they face.

BILL SMITH, APR, is principal of Smith-Phillips Strategic Communications and contributing editor of *The Parking Professional.* He can be reached at bsmith@smith-phillips.com or 603.491.4280.