By Jeremy Rock

So you're compliant – now what?

Not that long ago we were focused on educating the industry about becoming PCI compliant. We informed about the risks associated with being breached and let hotels know that it's not if you will be breached, but when. Stories were plentiful from many hotels, resorts and companies who were breached, and the efforts taken to become compliant and secure networks and data. All along there was a consistent message that this is something that needed to be vigorously maintained and that at no point could properties and companies become complacent in their efforts.

Unfortunately, there were some properties that were breached and treated PCI compliance as though it was a one-time effort. While time, money and resources were invested into the initial security of their networks and completed the required AOC (attestation of compliance), they did not invest in the required ongoing maintenance needed to maintain these security initiatives. The result is that we are starting to hear of properties that are being breached for a second time and they are starting to question how this could happen. While some of the breaches were attributed to advanced cyber-attacks, most were attributed to controllable reasons.

Changes in IT Personnel

There has been a change in the industry to reduce the level of IT support at the property level. While some of this is attributed to the economic downturn, other reasons include the move to SaaS or cloud-based applications. In the process, properties have lost key IT resources who were familiar with the networks and applications, as well as the security initiatives that were implemented in remediation to ensure PCI compliance.

Of further concern is the lack of hands-on IT resources that are familiar with the technical requirements for managing PCI compliance. The economy is picking up and hotels are hiring qualified resources away from competitors, leaving the original properties exposed due to the lack of experienced personnel. The knowledge loss of a specific property's network, applications setup and support requirements can be devastating to the PCI compliance efforts and difficult to replace in a timely manner. Oftentimes the replacements are not as technically skilled and the lead times involved with getting them "up to speed" can be considerable. The loss of qualified personnel leaves the property's PCI compliance efforts stagnant and exposed to additional breaches.

Ongoing Compliance Efforts

Many properties have exposed themselves to security breaches as a result of the lack of ongoing compliance efforts such as ongoing file monitoring, intrusion detection and maintain effective antivirus programs.

New Sophisticated Malware

We are also hearing of new malware that is far more sophisticated than the earlier rudimentary versions that were attacking the industry. These are proving to be much harder to detect and prevent than the earlier versions.

What can be done to limit or prevent properties from being breached?

- Remove credit card data from the property level through the use of encryption and tokenization.
- Continue the use of third-party monitoring services and applications such as file monitoring and intrusion detection.
- Maintain antivirus software and security updates.
- Ensure that network and firewall changes are not made without approval from network security personnel.
- Ensure that third-party authentication is used for all remote access support or other requirements.
- Conduct regular network scans to ensure that the network is sound and that there haven't been changes implemented that could compromise the security of the network.
- Maintain and enforce a vigorous password policy program.

New Malware

An examination of some of the new malware that is starting to infiltrate property's networks reveals that the bad guys are getting more sophisticated in their techniques and approach. An example from a recent breach showed that the malware entered the network as a Trojan virus and was undetected due to the way that it manipulated the workstations and servers. Effectively, once it was embedded, it was able to rename the drives so that when the installed antivirus scan ran, the scan was targeting a drive that did not exist. It's important to note that the malware was able to rename the drives even though the computer was still running. Observing the payload, it was programmed to intercept traffic coming in and out of the local network and was looking for number strings that included social security numbers, credit card data and login information. It is also important to note that in one particular instance the property did have a third-party monitoring and intrusion detection service in place. However, because nobody was monitoring the notifications internally, these expensive security solutions laid dormant, allowing credit card data to be potentially compromised.

- Implement and manage a security management hierarchy by assigning the minimum roles of compliance officer, compliance manager and compliance associate.
- Invest in training programs that adequately prepare security teams to manage compliance at all levels.
- Continue to look within the hospitality industry for qualified technical resources as outside resources tend to lack the knowledge and expertise of the hotel communications infrastructure.

Properties must remember that data security is still a very big threat to the business entity and that the financial impact and fallout from a security breach can be exceptionally costly, especially the second time around. There are initiatives underway to remove credit card data from the applications and property level with a number of gateway providers offering tokenization solution options that should be evaluated and, when possible, considered for implementation. Those entities that do not have the necessary security experience in-house should seek the advice and assistance of companies that specialize in providing these services. Hotels that are exposed or breached for a second time can expect to be subjected to severe fines and will probably be required to undergo stringent compliance efforts involving regular internal and external scans by certified QSAs and comprehensive reporting requirements.

JEREMY ROCK *is the president of the RockIT Group, a technology consulting firm specializing in new development and refurbishment projects. He can be reached at jrock@rockitgroup.com.*

Removing Credit Card Data from the Property

The movement to ensure compliance is the removal of credit card data from the property site. This is typically facilitated through the use of tokenization, the process of exchanging card data with a token at the point of swipe and storing the credit card data on the gateway processors system. With tokenization, the merchant maintains no credit card data at the property or at their application hosting sites. As such, even if the property's systems are breached, the exposure of credit card data is significantly reduced, if not eliminated, as the credit card data is not stored locally. With no card data present in many cases, hotels are therefore classified as SAQ "C" and the scope of PCI-DSS Compliance is significantly reduced. Thus, hotels and resorts are protected to the highest level of security available and their customer's credit card information exposure is significantly reduced, if not eliminated.

While much has been made of properties adopting a strategy of implementing tokenization, the number of properties that have actually deployed a comprehensive solution has been rather limited.

One property that recently decided to implement a fully tokenized solution is Bacara Resort and Spa in Santa Barbara, Calif. Under the direction of RockIT Group's IT consultant Scott Appleberry, the property installed is one of the first fully tokenized solutions involving Shift 4's 4Go and tokenized gateway applications on each of the property's POS applications which include Micros Opera, Micros POS and Par Springer-Miller's SpaSoft.

One of the most common problems with encrypting credit card data at the swipe is that it needs to communicate with the encryption application, which typically resides on a server on the network and there is potential for the data to be intercepted while communicating between the POS/reservation application and the encryption server. To limit the potential data exposure, Appleberry decided to setup the Shift 4 Universal Transaction Gateway (UTG), which encrypts the data on each of the respective POS servers. Micros POS and 4Go tokenize at the point of swipe on the terminal itself offering the highest level of security available today.

Bacara Resort and Spa believes that their move to eliminate all of the credit card data from the property will significantly reduce its exposure to breaches and allow guests to transact with the utmost confidence.