PCI COMPLIANCE

What Every Hotelier Should Know and Do

Payment Card Industry Data Security Standard (PCI DSS) compliance has become a very important consideration for hotels. Some hotels are not in compliance and don't even know it. There are significant penalties associated with non compliance including lawsuits, audits, fines and even losing the ability to process credit card payments.

Some may think that PCI compliance is about network and computer security, which it is. But, it is also much more, such as securing paper documents, proper shredding of documents and document retention, just to name a few.

Mike Seymour is vice president of operations and CFO of Postec, an Atlanta-based reseller of MICROS and IBM point-of-sale systems. Seymour is an expert on PCI compliance and offers the following insights. Among the items he describes are the use of validated applications, network security and physical security.

Network segmentation and the use of firewalls is very important. No email or Web surfing should be done on the secure side of a network.

A self assessment questionnaire should be used for smaller hotels and a PCI audit firm can be used to assist medium and large hotels. Liability for breaches falls on the hotel because of the credit card merchant agreement.

According to Seymour, the best source of information on compliance is found at www.pcisecuritystandards.org.

Hotels should click on the merchants link to find detailed information on compliance. The introductory page notes that enforcement of merchant compliance is overseen by individual credit card brands, not by the council itself.

There is a link entitled, "How to be compliant," that has additional links to each credit card brand.

There a three levels of validation:

- Self assessment questionnaire
- Onsite security audit
- Network scan

There are security policies for more than just merchants. Visa, as an example, recently published a Best practices for Payment Application Integrators and Resellers, which can affect hotels that have older equipment. Older versions of software may not be validated applications, that is, not meeting current security standards. This software must be updated immediately as part of overall compliance. Other vendor requirements include more secure networks, logins and restricting what personnel accesses certain systems.

Visa also published a bulletin in late 2007 that is directed toward credit card acquirers/processors that affects merchants (hotels). Acquirers are not permitted to process data from merchants that have vunerable payment systems. In addition, new payment applications must be validated against Visa's standards. These standards can affect both point of sale and property management systems, although the major vendors are in compliance. Visa continues to monitor all credit card processing applications, and those found to not be compliant will be denied access to the processing network.

There are levels of merchant compliance. A level 1 merchant processes more than 6 million transactions annually. This level requires an annual onsite security audit and quarterly network scans.

Level 2 merchants process between 1 million and 6 million credit card transactions annually. This level requires an annual self assessment and quarterly network scans.

Level 3 merchants process between 20,000 and 1 million e-commerce transactions annually and have the same compliance requirements as level 2.

Level 4 merchants process fewer than 20,000 e-commerce transactions a year and require annual self assessments and network scans.

Data security breaches can cost a hotel an average of $182 per compromised record. This does not include the cost of defending a lawsuit, if one is brought, or fines for non-compliance from individual credit card brands.

There have been some criticisms of PCI compliance. Some security experts have said that PCI compliance outlines just a minimum for security. These experts cite some requirements as being vague and subjective, thus subject to interpretation, both in implementation and enforcement. Others cite the high cost of implementation.

However, Visa has maintained that no compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach.

Being non-compliant can become a huge problem for a hotel. Make sure that all systems and policies are up to date.

Geoff Griswold *is a field engineer and general manager of the Omni Group, an IT services company specializing in the hospitality industry. He can be reached at (678) 464-2427 or geoff@atlantaomnigroup.com.*

Hotels are required to adhere to the following:

- **Build and maintain a secure network,** including the use of a firewall.
- **All passwords must be unique** to the hotel, not the defaults.
- **Protect cardholder data from unauthorized access**, both electronically and physically.
- Manage security issues and **keep antivirus and antimalware programs up to date.**
- **Restrict physical access to sensitive information**, including to filing cabinets containing paper forms. Do not store cardholder information in an insecure area.
- **Protect the transmission of cardholder data** including encryption of all transmissions.
- **Monitor and test all access to networks and cardholder data.** Change passwords regularly and deactivate passwords of terminated employees.
- **Have security policies in place** that are regularly reviewed and strictly enforced.