

by Dorian Cougias, Cihan Cobanoglu



© 2008 iStockphoto LP

# 7 Deadly Myths and Solutions for PCI Compliance

The first Payment Card Industry Data Security Standards (PCI DSS) Compliance in Hospitality Conference has reconfirmed what we found in our survey of hotel and restaurant managers; there is a big misunderstanding of PCI DSS within the hospitality industry. Below you will find the results of our survey and the seven deadly myths regarding PCI compliance.

## PCI Hospitality Survey

We have conducted an extensive survey of hotel and restaurant managers about PCI DSS compliance. The first question we asked operators was whether or not they believed their establishment to be fully compliant with PCI data security standards. Nearly 80 percent said yes. But when we drilled a little deeper and began asking respondents about the 12 specific requirements, a much clearer picture emerged:

- Only 40 percent regularly test their security systems and processes.
- More than 30 percent use vendor-supplied passwords (i.e., admin/admin).
- Only 41 percent track and monitor all access to network resources and cardholder data.

These facts show that many hotel and restaurant managers think that they are compliant while in fact they are not. There is no such thing as being partially compliant.

This is a very serious problem which many hospitality operators do not realize. We are beginning to witness a series of lawsuits surrounding not only the loss of credit card data, but personally identifiable information as well. We know that both restaurants and hotels (even the smaller level 3 and 4 merchants) are facing stiff PCI-related fines. In addition, there are court cases such as the one where Falcon Physician Reviews, Inc., filed suit in Dallas against Younan Hospitality Group LBJ Dallas, L.P. which owns Holiday Inn Select North Dallas.<sup>1</sup> The lawsuit alleges negligence in handling confidential private information and breach of contract that took place between September and November of 2005 after students and teachers

stayed for several weeks at the hotel.

The major problem that we found in both restaurants and hotels was that the operators simply do not know their responsibilities when it comes to PCI compliance. They think that this is somebody else's responsibility. That somebody else is either a vendor or credit card payment processing company. However, all parties involved in handling, processing and storing a credit card and credit card holder information have shared responsibilities. The ultimate responsibility in a hotel or restaurant lies with the operator.

## 7 Deadly Myths

**1 I am a small mom and pop bed and breakfast or restaurant. So, I am not part of, or don't have to comply with PCI DSS.**

This is one of the biggest myths of PCI DSS. Any merchant, regardless of size, is subject to PCI DSS in the moment that it accepts a credit card. If your establishment accepts credit cards, then you have to comply with all standards. However, if you are a level 4 merchant (less than 1 million credit card transactions a year), then you might not have to validate compliance (yet), but you still have to be in compliance with PCI DSS.

**2 I have a small business; hackers will not target my establishment. They will go after big guys, therefore, I do not have to worry about PCI DSS compliance.**

According to Visa Inc., small (level 4) merchants account for over 80 percent of compromise events. Hackers love small businesses because they are usually not well protected. Regardless of size, any organization that is not protected will be a target for hackers. The analogy is similar to leaving your car, luxury or a

regular car, on the street running with keys inside. A thief will come and steal your car. Protect it.

### **3** I have a firewall, so I really can't lose credit card or personally identifiable data.

Many POS systems store cardholder data as well as the personally identifiable data for your staff (such as name and driver's license or name and social security number). If you send your POS systems out for repair with that data on them, and they get lost (or replaced without wiping the data) – then that is a security breach that must be reported, and might even possibly need to be reported to state officials as a part of losing personally identifiable information. The news is filled with laptops and other devices that have been lost or stolen. Any device that held cardholder data (or personally identifiable data) that was lost or stolen or re-purposed without first wiping the data must be reported.

### **4** PCI DSS is only good for credit card companies. It has no benefit for my business.

PCI DSS is good for everyone. It is a win-win for all parties involved. These parties include you, the operator. By complying with PCI DSS, you will have a better IT infrastructure; better policies, network security, physical security and will protect customer and staff data better.

### **5** I asked my vendor and they told me that my system is PCI compliant. I do not have to do anything else.

We wish it was that easy. Even though your vendor

may be 100 percent PCI compliant, there are still several things you have to do as an operator. For example, it is your responsibility to change the vendor-supplied passwords. More than 30 percent of hospitality companies use vendor-supplied passwords (i.e., admin/admin).

### **6** PCI DSS is so complicated that as a small business owner, I will never get there.

You can be 100 percent compliant no matter how small or big your company is. You just have to make smart decisions. If you do not need it, do not store the data.

### **7** I am alone in this. There is no support for me. Where do I start?

You are not alone in this. There are many resources available for you. The first place to start is the actual PCI DSS. Go to: <https://www.pcisecuritystandards.org/> and read the DSS. Visa has extensive information for their CISP at [http://usa.visa.com/merchants/risk\\_management/cisp.html](http://usa.visa.com/merchants/risk_management/cisp.html).

*Dorian J. Cougias is the co-founder and primary architect of the Unified Compliance Framework, the first and largest independent initiative to map IT controls across international regulations, standards and best practices. He is currently an adjunct professor at the University of Delaware and the lead analyst at Network Frontiers. Cibac Cobanoglu, PhD, CHTP, is an associate professor of hospitality information technology at the University of Delaware and manager of eXperimental Guestroom (X-Room) at the Courtyard Newark.*

(Footnotes)<sup>1</sup> <http://www.lawcash.com/attorney/4874/younan-hospitality-group-holiday-inn-select-dallas-north-lawsuit.asp>

# Simplify™ PCI

## Shift4 Corporation

Daniel Montellano  
Manager, Business Development, Hospitality  
(702) 597-2480 ext. 43100  
[dmontellano@shift4.com](mailto:dmontellano@shift4.com)

[www.shift4.com](http://www.shift4.com)

[www.simplifypci.com](http://www.simplifypci.com)