



Vendor Safe
Technologies

"your one stop shop for PCI compliance"

Whitepaper

Control Your Security, and PCI will Follow

The four most vital actions restaurants can take to accelerate network – and credit card data – security

by Bradley K. Cyprus, Senior Security Architect, Vendor Safe Technologies

June 2008





Vendor Safe Technologies

"your one stop shop for PCI compliance"

In recent years, it seems that there has been a concerted media effort to warn the public about credit card and identity theft. What seems to be lost in those stories, until you do a little digging, is how often identity theft can be traced back to brick and mortar establishments that accept credit cards. In the news most recently was Dave and Busters, which had 11 locations compromised by hackers using malicious software to steal credit cards from their network. Several other major security breaches have made headlines over the last year, including (restaurant), (restaurant), and (restaurant).

This is not surprising, since the "2008 Data Breach Investigations Report," published by Verizon's Business Risk Team, reports that over 57% of all breaches in security that resulted in identity theft took place at retail, food service, or hospitality establishments. Sources at Visa have reported similar findings. The National Restaurant Association notes that the sheer volume of people who eat at restaurants could account for the high volume of thefts. Regardless of the underlying rationale, there can be little doubt that restaurants are a prime target for hackers and other electronic criminals.

April 2007 marked the end of a professional computer hacking ring that was working out of Manhattan and Eastern Europe. This professional group of thieves targeted over 40 restaurants during their 17-month operation. Before 12 out of the 13 criminals were indicted, they had orchestrated extensive collusion with internal employees and cyber attacks from external sources to help them steal credit cards from unsuspecting diners across the Eastern Seaboard of the U.S. In the short period of time that they were operating, they managed to illegally charge \$3 million on the stolen credit cards. *The negative consequences resulting from credit card data theft is detrimental to any establishment. It can easily be fatal to those with limited financial resources.*

When a popular merchant has its credit card data compromised, the media engage in a feeding frenzy, highlighting the dangerous practices that were responsible for the breach. Articles describe how the problem could have been avoided, and the issue becomes a permanent record on the Internet, available for anyone with a computer to scrutinize. Besides the media attention, real, live patrons are affected by a breach. At a minimum, they are inconvenienced with replacing their credit cards. In extreme cases, they have the monumental task of clearing their credit history and disputing charges because the hackers managed to buy so much under their name. One thing is for sure: They will be angry at the establishment that caused them their headaches. Word of mouth is a two-way street. Just as a great meal will get a satisfied customer talking around the water cooler, identity theft will make that same patron a poison pill, spreading their dissatisfaction and annoyance across their entire circle of friends.

Recognizing the potential problems associated with network security, the major credit card companies have worked together to create a security standard with which merchants must now comply. It is known as PCI-DSS (Payment Card Industry Data Security Standard). This is the method that the industry is using to force merchants into protecting their locations with information technology best practices. The intent of the standard is to reduce credit card theft and to help keep consumer confidence in the credit card industry as a whole.

The negative consequences resulting from credit card data theft is detrimental to any establishment. It can easily be fatal to those with limited financial resources.



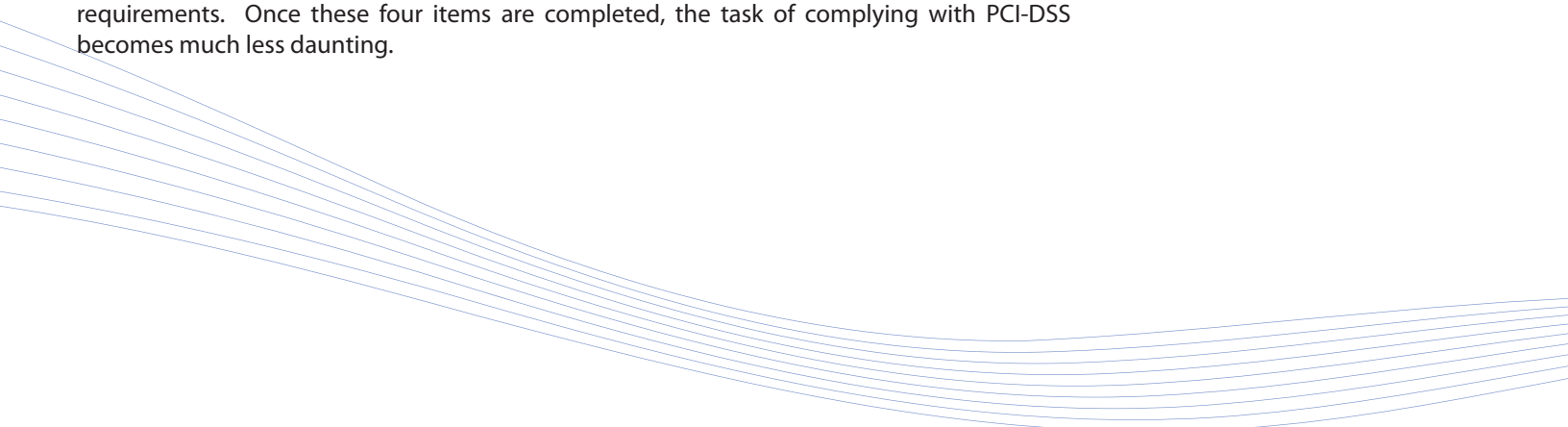
Since the inception of PCI-DSS in 2004, credit card companies have become increasingly more demanding on merchants to conform. Compliance to this standard is no longer optional for any merchant, big or small. The credit card companies will impose fines for lack of compliance, and merchants will be responsible for the costs associated with a breach. Total costs to a merchant include a forensic audit to determine how the breach occurred; fines from the credit card companies for failing to comply with PCI-DSS; a formal security audit to verify future compliance; legal fees stemming from the inevitable law suits brought on by the credit card holders; card replacement fees for each re-issued card; and the loss of good will due to the negative publicity. Conservative estimates place the total cost of noncompliance to a small merchant at well over \$100K. With the frequency and magnitude of these thefts increasing, network security is a requirement that a responsible restaurateur must take seriously. It benefits the customers of the secure establishment, and *the financial risks associated with a breach outweigh the costs of solving the issues, since low-cost solutions are now available to merchants.*

the financial risks associated with a breach outweigh the costs of solving the issues, since low-cost solutions are now available to merchants.

So why have merchants been so slow to adopt additional security? In a nutshell, most dining establishments are in the business to sell food and not maintain computer security. Parts of the PCI-DSS standard are hard to understand, and some of them require a change in operations. The bottom line is that the standard will only become stricter as new hacking methods are developed, and each establishment must become PCI-DSS compliant. For merchants looking for a good place to start, four imperative actions will get you started on PCI compliance and help shore up many of the most common vulnerabilities found on computer networks today:

1. Do not allow unsecure access from the Internet or wireless networks to your computers.
2. Block internal computers and data transfer protocols from the Internet except to the sites and ports necessary for business functions.
3. Make sure that the POS software storing credit cards is secure.
4. Make sure that level of security in place is verifiable for mounting a defense.

This is only a short list of computer security and it does not cover all of the PCI-DSS requirements, but each of the proceeding suggestions are integral components of the PCI-DSS requirements. Once these four items are completed, the task of complying with PCI-DSS becomes much less daunting.





Action #1 – Do not allow unsecure access from the Internet or wireless networks to your computers.

If someone can run remote access software like PC Anywhere or VNC (even if an additional password for access is required), then hackers might be able to break into the associated program's data port that is publically available. This is the most common method that hackers use to gain access to improperly segregated networks. Secure networks do not allow traffic from public networks to access servers containing confidential data, including servers processing credit cards. If remote access is necessary from a business perspective, then keep that communication secure. For example, you could set up a Virtual Private Network (secure and encrypted network connection that effectively makes a public network, the Internet in this case, safe for remote access).

Wireless networks must be secured to the same degree as Internet connections. If a location has a Hotspot that patrons can use to browse, then it is up to the merchant to ensure that a firewall actively separates that public traffic from the credit card processing network. In the case of wireless POS terminals, the merchant must implement encryption techniques that are strong enough to keep hackers from gaining access to the private network through the wireless connection. In simplest terms, a firewall must block, monitor and log data transmission from every wireless network so that hackers are thwarted from gaining access to sensitive data.

Action #2 – Block internal computers and data transfer protocols from the Internet except to the sites and ports necessary for business functions.

Access to the Internet must be limited. Malware (malicious software) and hackers posing as legitimate employees may try to copy sensitive credit card data from inside the location and send it to another server on the Internet. At a truly secure location, this will not be possible. One way to accomplish this, and PCI-DSS requires it, is for a firewall to block unauthorized data transmission to the Internet. Since credit card data is valuable to hackers, merchants need to treat their back office computers like precious commodities. Those systems do not need access to the entire Internet. In fact, most back office servers at restaurants can get away with only being allowed to communicate to their credit card processors, browse their food supply vendors, and possibly access a corporate logistics site. By contrast, it is irresponsible for that computer to have unrestricted access to the Internet.

Action #3 – Make sure that the POS software storing credit cards is secure.

The POS (Point of Sale) application software that processes credit cards is the central repository for the data that hackers want to steal. If the software itself does not protect the data internally, then a hacker's job is that much easier. The good news is that the PCI Security Standards Council (www.pcisecuritystandards.org) maintains a list of secure software as does Visa (www.visa.com). If only approved software is used, and if it is installed in the manner intended by the manufacturer, then the data stored in the software will be difficult for hackers to compromise. Non-validated software should be either upgraded or replaced with packages that have been tested and certified for their security. While it will most likely cost money to upgrade to a safe package, a secure starting point is necessary when trying to thwart hackers on a network.

Action #4 – Make sure that the level of security in place is verifiable for mounting a defense.

If a suspected breach of security must be defended, a merchant will need to be prepared to stand before an acquiring bank or a credit card company such as Visa. If the merchant is using a home-grown solution, he will be performing this task. If the merchant's security is part of a managed package provided by a security vendor, then that vendor should perform this role. Either way, in validating the security measures at a given location, the merchant must provide to authorities a wealth of information, including:

- Network diagrams
- Security access logs
- Firewall logs



Conclusion

In the PCI-DSS standard, there are many components to logging and documentation. Some of them are complicated to implement. As a simple first step in obtaining much of the data that needs to be stored, a merchant needs to ensure that the security measures implemented at a location provide a convenient way to store and retrieve critical data for at least a year. The technical sophistication necessary for this suggestion surpasses the resources available to many merchants, but several POS resellers and other third parties such as Vendor Safe have options in place to assist with this crucial security practice.

The end result of implementing the four actions highlighted in this paper is that most hacking attempts will either fail or require more effort than makes sense from a cost analysis standpoint. No level of security will ever make a system completely hacker proof because given enough time, determination and hard work, any security can be compromised. *The important thing to remember is that hacking is a business to the criminals who participate in it. They have to weigh the risks and rewards before they invest the resources in an attempt to commit a crime.*

Given two identical networks, one with properly configured security devices, logging, and active blocking at the Internet and its twin network with no such security, it is easy to understand why a hacker would target the unprotected system. The potential payoff is the same, but the reduced effort and risk of hacking into the unprotected network makes it the target of choice.

While it is important to note that someone implementing the actions suggested in this paper will not meet the PCI-DSS requirements, they are components of PCI-DSS that will have the most immediate impact on the overall security of any network. The other components of PCI-DSS, including policy and procedures, physical access, change and control documentation, and other details, are required for every merchant to be compliant, but by focusing on the hardest technological challenges first, merchants will be able to quickly shore up most of their vulnerabilities and subsequently work toward compliance with the full standard.

The Vendor Safe Solution

Vendor Safe's PCI Managed Security Suite™ is a one-stop, affordable solution for PCI compliance. With implementation in less than 30 days, merchants can immediately realize the benefits of improved security. The solution counters the three most common ways in which merchants are breached:

- Penetration of the internal network by hackers via the internet,
- The covert installation of a device on the internal network that scans for all number sequences that match a credit card format, and
- File transfer of cardholder data from the internal network to a remote location, usually a foreign country.

The important thing to remember is that hacking is a business to the criminals who participate in it. They have to weigh the risks and rewards before they invest the resources in an attempt to commit a crime.