Five PCI Security Deficiencies of Restaurants

The Most Common PCI Compliance Mistakes of Brick-and-Mortar Locations

By Bradley K. Cyprus - Chief of Security and Compliance, Netsurion

The five major credit card brands (Visa, MasterCard, American Express, Discover and JCB), joined forces in 2004 to create the Payment Card Industry Data Security Standard (PCI DSS). Its sole purpose is to assist merchants in building a security program that meets the requirements expected by the card brands.

Since then, businesses have been scrambling to make their systems PCI compliant. Many have made great strides in making credit card transactions more secure. However, five common shortcomings often throw the PCI compliance efforts of brick-and-mortar restaurants and retailers off track. This paper will discuss those deficiencies and provide some general guidance to overcome them.

1. Insecure Remote Access Without Two Factor Authentication

Remote access is the process by which someone who is not physically located at a computer uses electronic means to make a connection to that computer. A common example would be a restaurant chain's regional manager in a hotel room accessing reporting data online from a server in another physical location. In most cases, the remote access either connects to the data, as in a remote login to a server, or it initiates a session, which in essence emulates direct access to the remote computer's keyboard and mouse. Inevitably, when a credit card breach story makes the news, somewhere in the details unauthorized remote access was part of the issue. The major problem for retailers is that remote access is usually necessary from both an operational perspective and for efficient system support.

Modern Point of Sale (POS) software has reporting capability that is useful to operators in measuring the performance of a given location. Accessing those reports off-site increases the speed at which the data is obtained, and in the case of a multi-unit franchise, a single person can remotely analyze the business metrics for the entire organization, without ever leaving the home or corporate office. Furthermore, software support and training can occur as needed without sending technicians on-site. Support staff can remotely take over a computer and perform their duties without the delay or expenses associated with travel. Savvy businesses rely on this technology to improve their operations.

The problem associated with remote access is that electronic data thieves make their living by penetrating networks that have this technology enabled. Businesses are moving their electronic communications to the Internet, and that includes remote connectivity. Hackers have numerous techniques to circumvent security measures. If they can communicate directly to a POS server that stores credit card data, it is only a matter of time before they will be able to breach the location and steal card information. Recognizing these vulnerabilities, PCI requirements include several measures for securing remote communication.

Requirement 1.2 and 1.3 of the PCI standard prohibit untrusted networks or unnecessary communication to the cardholder environment. This is to limit the external connections that are allowed into an environment that accepts credit cards. In addition, requirement 8.3 of the standard demands that two-factor authentication is implemented for all remote access to the POS network.

In short, two-factor authentication can be thought of as something a user knows and something the user has that will conclusively validate the identity of the person logging into the network. Usually, the part that a user knows, the first factor, is a username and password. Without the second factor, if that information was ever compromised, someone else could use those credentials to log in. Therefore, the second factor guarantees that someone accessing the network is actually who they claim to be. It cannot be more information that a user knows. It should be something physical such as a fingerprint, a token, an individual SSL certificate, or something else unique to the individual. Newer approaches use a random six digit number sent to a cell phone or email account, the number is keyed in to a field below the user name and password and is typically good for two minutes.

Meeting the PCI standards can be daunting for merchants with limited technological capabilities, but it is critical for running a secure business. Protecting remote access is crucial as part of a business security plan, and merchants must find a solution that meets their needs while keeping the credit cards processed on their network secure.

2. Open Wireless Networks

Open wireless refers to networks that have wireless communication, typically using a wireless Ethernet or Bluetooth, with insufficient protection to prevent unauthorized entry into the POS environment. Unlike the wired equivalent, wireless networks have radio receivers, called access points that must accept packets from any computer that transmits to them. Access points can be configured so that unauthorized machines will not be allowed to send data, but the access point must evaluate every attempt made by a computer to access the network. Furthermore, the radio traffic of a wireless network can be intercepted by anyone with a wireless interface card (WIC).

Because sensitive data may be transmitted in this manner, POS environments utilizing wireless networks need to encrypt the communication so that it remains private and is not stolen during the credit card transaction. When data is encrypted, it is transformed using a mathematical formula and a variable code, known as a key. If someone intercepts the encrypted data, they will not be able to use it unless they also obtain the key necessary to decrypt it. It is therefore critical that they key is protected to thwart any attempts made to steal sensitive data.

PCI devotes much of its focus to the wireless environment and how it relates to the POS network. Requirement 1.2.3 demands that a firewall separate a wireless network from the cardholder data environment. This means that if a wireless device is used for business needs outside of processing credit cards, it must be segregated from the rest of the network. If wireless communication is used in the processing of credit cards, PCI requirements 4.1 and 4.1.1 dictate that strong encryption be used to protect the transmission of that data. Lastly, PCI calls for a wireless detection process in requirement 11.1 to ensure that no one secretly adds a wireless access point to a network that would enable a thief to steal data over the air.

The benefits of wireless communication, particularly in hospitality, are clear from a business perspective – faster order entry and tableside credit card processing to name just a few. Also, many restaurants benefit from offering a public Internet connection using an in-store wireless network. If a business decides to embrace this technology, then it is the responsibility of that merchant to ensure that the wireless communication is set up so that customer data is not compromised. All retailers must concern themselves with this security on their wireless networks, and if they cannot manage the technology internally, then the only responsible decision is to bring in the appropriate expertise to secure the environment.

3. Insufficient or Poorly Managed Firewall

If a merchant has an Internet connection, that communication should be managed by a firewall. By definition, a firewall is a device that allows or prohibits certain types of communication based on a set of criteria, commonly referred to as a rule set.

The firewall can be thought of as the device that acts as the gatekeeper between the public Internet and the private cardholder data environment. In the typical merchant environment, the firewall is the first line of defense against external threats. It is responsible for blocking inbound Internet traffic, including the attempts of hackers to penetrate the network. A properly configured firewall can also help a merchant from accidentally causing an internal issue by blocking access to the Internet from within the POS environment. The problem many businesses face is that not all firewalls are created equal, and the rule set is only as good as the individual – hopefully a security expert – who set up the protection.

PCI DSS devotes the entire first section of the standard to firewall security and the methods that should be employed when trying to protect a merchant location. The top level name for Requirement 1 of PCI is, "Install and maintain a firewall configuration to protect cardholder data." Every sub-requirement in the first section has at least something to do with properly maintaining the firewall in the network. The other 11 Requirements of PCI include over 25 additional mandates that directly pertain to implementing and maintaining a secure firewall. It is one of the most heavily referenced components in PCI.

There is a reason that the PCI standard starts with firewall security. Without good protection at the Internet connection, almost all other measures are irrelevant. Hackers rely on poorly configured firewalls when they begin their attempts to violate network security. For example, if a firewall allows direct communication from the Internet to the POS Server, then a cyber thief might be able to employ various techniques to circumvent the other protections afforded by the server. In the same vein, if that same POS server is allowed unrestricted access to the Internet, than it might be possible for a merchant to download malicious software whose sole purpose is to steal sensitive data. Retailers must not underestimate the importance of properly implementing and supporting their firewalls. Those who allow inadequate protection to creep into their network face the distinct possibility of a catastrophic breach of their data.

4. Out-of-Date Point of Sale Software

When PCI was introduced in 2004, the POS software industry had to face the fact that their products made it too easy for credit card thieves to steal data. Many POS software packages stored credit card data much longer than was necessary from a business perspective. Their databases were not encrypted properly, allowing credit card data to be read directly out of them. When PCI was adopted, POS software companies rewrote their software to comply with the standard and released updates so that merchants would be able to keep their data secure.

By this time, most companies have released compliant software, but it is up to the merchants to upgrade their systems accordingly. If a location has insecure software managing credit card transactions, then that business is a prime target for cyber thieves. Even with all of the recent industry education efforts and information available about credit card breaches, many merchants have elected to ignore the threat and continue running their stores with insecure software. It is usually a matter of inconvenience or expense that drives merchants to delay this critical upgrade, but the issue is too important to ignore. This problem has been exacerbated recently since one of the most popular operating systems, Microsoft Windows XP, is no longer supported. Now, merchants must not only worry about keeping their POS software up to date, but the viability of the underlying operating system must be examined as well.

Because vulnerable software is so alluring to hackers who are looking to steal credit card data, the PCI standard devotes much of requirements 3, 4, 6 and 8 to the installation and maintenance of compliant software. There is more in the standard about securing POS software than any other single network component. POS software companies write their products to a specific software standard called the Payment Application Data Security Standard (PA-DSS), which gives them a means to validate that their offerings meet all the software requirements of PCI.

The industry, in general, has recognized that the applications used to process credit card transactions are a key component in maintaining a good security plan at any particular location. The companies that write this software have spent the last several years updating the internal security in their packages to help protect this sensitive data. It is up to the merchants who have the trust of their patrons to do their part and update their out of date POS systems with modern ones that take data security seriously.

5. Educating Credit Card Handling Staff and Management

While implementing security, too many businesses focus on the technical aspect of the network, discounting the importance of user education. People are often the weakest link in a security plan. By taking the time to incorporate the elements of PCI security, businesses can increase the protection of their sensitive data without making any additional investment in their infrastructure.

PCI is clear on the importance of training. An element of requirement 12 specifically acknowledges that card handling employees must receive credit card security policy updates annually. This makes sense, given that these employees are typically the ones who have the most physical access to the credit cards of patrons. If they are violating the best security practices of an organization, then it does not matter how secure the remainder of the system is. Good security must become a part of the corporate culture of a business, and that process begins with a training program.

There are numerous other ways in which merchants can educate their staff. Regardless of how an organization chooses manage training, it needs to be an ongoing initiative so that there are no gaps in an otherwise sound environment.

7324 Southwest Freeway
Suite 1700, Arena Tower II
Houston, Texas 77074

P: 713.929.0200
F: 713.541.1065
Netsurion.com