A guide from FastCasual.com

Frequently Asked Questions about PCI Compliance

A credit card data breach can put a restaurant operator out of business. PCI compliance can help avoid those breaches, but it's only one part of the security process. Learn what restaurant operators need to know to ensure compliance, including initial steps, pitfalls to avoid and how to develop a culture of security.

Developed and published by

FastCasual.com
insights for innovative restaurants

Sponsored by

VendorSafe TECHNOLOGIES
Protect Data. Secure Business.

Contents

Frequently Asked Questions about PCI Compliance

About the sponsors

*For more than 20 years, **Vendor Safe Technologies** has been a leader in providing secure networks across widely distributed enterprises. Founded in 1989, Vendor Safe has earned the trust of customers for the unfailing ability to manage the business environment while delivering unsurpassed levels of data reliability and security. Today, its primary focus is providing secure networks and credit card data security services. Vendor Safe specializes in providing Payment Card Industry Data Security Standard (PCI DSS) solutions. Due to its scalability, the company delivers a solution that meets and exceeds many of the requirements for Level 1 through Level 4. Vendor Safe continues to provide Managed Virtual Private Networks (VPN) for enterprises, as well as deploying a proprietary platform enabling end users to deploy networks in an effortless fashion.*

*Since 1997, **FastCasual.com** has reported on the important news, events, trends and people in the $23.5 billion fast casual restaurant industry segment. The site reaches a global audience of industry professionals looking to track the latest food and beverage trends, top markets for growth and hot concepts. FastCasual.com features a directory of product and service providers as well as slideshows, videos and research.*

Published by NetWorld Alliance.

Written by **Richard Slawsky**, contributing editor, FastCasual.com.
Dick Good, CEO
Tom Harper, president and publisher
Joseph Grove, vice president and executive editor

Introduction

If any restaurant operator doesn't comprehend the importance of maintaining security when it comes to credit card information, the following example should help.

In the summer of 2010, the credit card system at Julie's Place was infiltrated by hackers who gained access to customers' card information. Dave Wendland, who owns the popular Tallahassee, Fla., dining spot, said the data breach has cost his business both financially and professionally.

Beginning in July 2010, customers began telling Wendland that their credit cards had been used out of state and in Europe. Wendland called his POS provider, who assured him that both his remote credit card terminal and Internet connection were secure.

Eventually, the financial crimes unit of the local sheriff's office contacted Wendland. Investigators estimate there were more than $200,000 worth of fraudulent charges made to customers' credit cards as a result of the breach.

There was evidence that intruders were able to get past the system's firewall and remotely access the restaurant's credit card terminal and steal customers' information.

Following the breach, Julie's Place underwent a forensic exam that cost more than $12,000. Sales at Julie's Place were down several thousand dollars per week in the months following the breach, Wendland said.

Wendland's experience serves as a lesson on the importance of PCI compliance and data security. Theft of customer data is on the rise, and the costs associated with a data breach could shut down a business.

"Twenty-three percent of the hospitality industry experienced a data breach in 2009, with restaurants and hotels accounting for the majority of cases," said Tim Horton, vice president of merchant product development with Atlanta-based First Data, a provider of credit card processing services.

"Threats are evolving as organized thieves use ever-more sophisticated techniques to hack into more merchants' or restaurant operators' systems to steal sensitive data," he said.

In this guide, sponsored by Vendor Safe Technologies, learn what PCI is, how business operators can become PCI compliant, pitfalls to avoid and where business operators can turn for help if the task becomes too daunting.

By Richard Slawsky, Contributing editor, FastCasual.com

Theft of customer data is on the rise, and the costs associated with a data breach could shut down a business.

Chapter 1 PCI DSS defined

Any business that accepts credit card payments is required to comply with the Payment Card Industry Data Security Standard (PCI DSS), created in 2004 to establish minimum data security measures for organizations around the world that hold, process or exchange cardholder information from any of the major card brands. These security measures are reviewed and revised on a rotating three-year schedule, and the latest version was released in October 2010.

"Long before PCI standards came into being, each of the major credit card companies had their own data security standards and they were all different," said Shekar Swamy, president and founder of Ellisville, Mo.-based Omega ATC, a specialist in data security and PCI compliance.

"So the five major card brands — Visa, MasterCard, Discover, American Express and JCB, which is the Japanese card brand — came together to form this PCI data security standard so that one set of standards could be adopted across all brands," he said.

Validating compliance depends on levels

The card brands define various merchant levels and the methods needed to validate compliance based on annual transaction volume and processing type. There are nuanced differences between all the major cardholders. Below are Visa's Merchant Levels.

Level 1: Any merchant — regardless of acceptance channel — processing more than 6,000,000 transactions per year requires:

- Annual on-site review validated by a Qualified Security Assessor (QSA).
- Quarterly network vulnerability scan validated by an Approved Scanning Vendor (ASV).

Level 2: Any merchant — regardless of acceptance channel — processing 1,000,000 to 5,999,999 transactions per year requires:

- Annual PCI Self-Assessment Questionnaire (SAQ) validated by the merchant. It is recommended to enlist the support of a QSA to assist in answering the questionnaire.
- Quarterly network vulnerability scan validated by an ASV.

Level 3: Any merchant processing 20,000 to 999,999 e-commerce transactions per year requires:

- Annual PCI SAQ validated by the merchant.
- Quarterly network vulnerability scan validated by an ASV.

Level 4: Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 999,999 transactions per year requires

- Annual PCI SAQ validated by the merchant.
- Quarterly network vulnerability scan validated by an ASV.

Any merchant that has suffered a hack that resulted in an account data compromise may be escalated to a higher validation level.

Source: Heartland Payment Systems

The type of measures a business is required to take depends in large part on the number of credit card transactions it processes each year. Organizations that handle large volumes of transactions must have their compliance assessed by an independent assessor known as a Qualified Security Assessor (QSA), while companies handling smaller volumes of transactions may demonstrate compliance via a Self-Assessment Questionnaire (SAQ).

The various SAQs are available for download at www.pcisecuritystandards.org. The Self-Assessment Questionnaire C, which is often the form restaurant operators must use for their compliance efforts, includes questions about network firewall configuration, data encryption and policy and procedures.

"Someone can purchase card numbers on the black market for $2 to $5 per card number," Swamy said. "Part of the reason for the development of PCI standards was to put the responsibility for data security back on the restaurant operators."

Most restaurant operators fall into the Level-4 merchant category, meaning they process fewer than 1 million transactions per year. Even though a restaurant chain may have thousands of locations in North America, those locations typically are operated by franchisees who own just a few locations.

And because Level 1 merchants, who process 6 million or more transactions per year, are already required to have stringent security measures in place, data thieves are finding it easier and more profitable to go after those smaller players, experts say.

"That is absolutely correct," Swamy said. "Even a midsize operator who owns 30 or 40 restaurants doesn't have the technological sophistication of the really large companies. The opportunity to steal information from these operators is greater and there are greater numbers of them."

12 steps to PCI

Much like food safety regulations, PCI requirements are important standards established to protect consumers. To achieve PCI compliance, owner/operators must meet these 12 requirements:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to data on a need-to-know basis
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor access to network resources and data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

Navigating all the PCI scans

	Intent	Goal	Common misconceptions
External vulnerability scans (ASV scans)	Check that public facing devices on the Internet are not vulnerable to known attacks or susceptible to exploits that hackers use to circumvent defenses on systems. Patching, upgrading or reconfiguring a system often is required after a scan fails.	4 passing **quarterly*** scans	• Passing an external scan does not mean that a location has no vulnerabilities. It simply means that it is not vulnerable to some of the common methods hackers use from the Internet to illegally enter a network without permission.
Internal vulnerability scans	Validate that the systems on the local network are not running with known vulnerabilities or insecure services that could be exploited to reveal cardholder data. Patching, upgrading or reconfiguring a system is often required after a scan fails.	4 passing **quarterly*** scans	• The external vulnerability scan does not include what is necessary for the internal vulnerability scan. They are two completely separate items. • Even though none of the card brands specifically require the individual internal vulnerability scans to be turned in for validation purposes (unlike the external scans which are often required to be turned in), merchants must still able to show that they are working to resolve any issues that the scans uncover. It is not acceptable to ignore "high" vulnerabilities that are listed in the internal vulnerability scan.
Wireless detection	Examine the local network to determine if unauthorized wireless access points have been added to the network	4 **quarterly** examinations (possibly scans) looking for rogue access points	• Wireless detection does not need to include wireless scans or wireless intrusion detection or prevention technology. The method used to look for wireless devices must be appropriate based on the complexity, size and individual circumstances of the cardholder data environment. Using technology to assist in this effort is a best practice, and it should be highly encouraged, but PCI acknowledges that a physical examination (assuming it is thorough enough to find rogue access points) could be an adequate measure to comply with this part of the standard.

*The scan must be repeated if the cardholder data environment undergoes a significant change.

How does all of this examination help a merchant from a practical standpoint?

- By removing vulnerabilities and insecure systems, cardholder data will be better protected.Do not use vendor-supplied defaults for system passwords
- These scan techniques are particularly crucial to smaller merchants. It is possible to limit the scope of an assessment using these scans (along with some other security requirements) to eliminate or at least reduce the complexity of the yearly penetration test that PCI also requires.

Tips and tricks for reducing the scope under PCI

As a merchant, it is always helpful to reduce the scope of PCI requirements. When something is in scope (a server that stores credit cards for example), it must meet all of the requirements as stated in PCI. When something is removed from scope, it is either exempt from PCI entirely or the security associated with that device is at least less critical. Two of the most touted (and occasionally overhyped) technologies that offer much in the way of minimizing the risks associated with credit cards are tokenization and point-to-point encryption. Both of these technologies can benefit a merchant from a security standpoint, and when they are implemented correctly, they can even help a merchant reduce the amount of effort required to achieve PCI compliance.

It is important to note that neither of these technologies can remove the full burden of PCI from a merchant. PCI includes technology, processes, operations, testing and validation. In fact, it is impossible to issue a blanket statement with any degree of accuracy about how much either of these technologies will actually impact the scope of PCI for any given merchant. Too many variables are involved, such as encryption key management, timing between swipe and transmission, token data recovery and many others. A good rule of thumb is that merchants who were once faced with filling out the highly involved Self-Assessment Questionnaire D (SAQ D), are able to reduce their burden and fill out the less cumbersome SAQ C. The manner in which these technologies are implemented is the key to reducing scope, so before leaping blindly into either tokenization or point-to-point encryption, it is important to have a security professional examine the proposed solution so that merchants can achieve their desired level of scope reduction.

Information courtesy of Vendor Safe Technologies.

Chapter 2 More than a checklist

While struggling to understand the importance of the Payment Card Industry Data Security Standard, many restaurant owners are putting themselves and their customers at risk by using a checklist approach.

"This is a misconception that nearly every restaurant operator we run into has," said Brad Cyprus, senior security architect with Houston-based Vendor Safe Technologies, a provider of security solutions.

"People think that PCI is a checklist standard that you just fill out, and that determines whether or not you are PCI compliant," he said. "That is the wrong way to be looking at PCI."

To fully protect data, it is best to approach PCI as a means to strengthening security, instead of simply meeting compliance standards, experts say.

If a breach occurs, the credit card companies will bring in their own investigators to determine what happened.

"If there's a confirmed breach, the more you have done, the better off you will be from a mediation standpoint," said Robert Kantor, director, information security and compliance at New Hartford, N.Y.-based PAR Technology, a provider of systems and service solutions for the hospitality industry.

"Having done due diligence can be beneficial if there is a problem," he said. "I think the penalties are going to be more severe and the remediation is going to be a longer road to get back to where you should be if you have ignored these things, if in fact you are still in business."

PCI is more than a checklist standard. Instead, it is a means to strengthening security.

Initial steps

With accountability growing, merchants are recognizing the importance of deploying critical services to protect cardholder environments. Despite the growing threat, however, many merchants have been slow to upgrade their systems and beef up security.

"Most dining establishments are in the business to sell food and not maintain computer security," Cyprus said. "Parts of the PCI DSS standard are hard to implement, and some of them require a change in operations."

Many locations running remote software have protected their data from Internet access while ignoring the threat posed by the wireless network they have installed as a matter of convenience for their patrons or their own operations.

For restaurant operators looking for a good place to begin, four actions can get them started on PCI compliance and help shore up many of the most common vulnerabilities found on computer networks today, Cyprus said.

No. 1: Don't allow unsecured access from the Internet or wireless networks to the computers.

The most common method hackers use to gain access to improperly segregated networks is via remote software. If someone can run remote-access software such as PC Anywhere or VNC, then hackers might be able to break into the associated program's data port that is publically available. 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.

If a location has a hotspot that patrons can use to browse the Internet, 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 the 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. Many locations running remote software have protected their data from Internet access while ignoring the threat posed by the wireless network they have installed as a matter of convenience for their patrons or their own operations.

Remote access software can leave a network vulnerable to hackers. Secure networks do not allow traffic from public networks to access servers containing confidential data.

No. 2: Block internal computers and data transfer protocols to 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. One requirement of PCI DSS is for merchants to have a firewall to block unauthorized data transmission to the Internet.

Firewalls can be a challenge to install, however, and cause a disruption in the business if not done properly.

Seek the assistance of a security specialist if the task is too complex to be handled in-house. There are solutions that small businesses can implement that are secure and affordable, and the technology is crucial to properly run a business in the

modern environment rife with cyber crime.

No. 3: Make sure that the POS software storing credit cards is secure.

The POS 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 PCI Security Standards Council maintains a list of secure software that was developed under an application standard called PA DSS. 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 either should be 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.

No. 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 homegrown 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.

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.

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

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 Technologies, have options in place to assist with this crucial security practice.

"The important thing to remember is that hacking is a business to the criminals who participate in it," Cyprus said.

"They have to weigh the risks and rewards before they invest the resources in an attempt to commit a crime," he said. "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."

Chapter 3 Pitfalls to avoid

Even with a restaurant owner's best intentions, there are still plenty of pitfalls when it comes to thinking about PCI compliance.

It can't happen here

The first pitfall to avoid when it comes to PCI compliance, experts say, is the belief on the part of business operators that a data breach or other fraud incident can't happen to their business.

"In reality, because of the number of internal and external fraud possibilities, every business is vulnerable," said First Data's Horton.

"A recent study conducted by the National Retail Federation and First Data revealed that almost two-thirds of respondents believe that their business is not vulnerable to credit/debit card data theft and 60 percent are unaware of the costs they could incur in the event of a breach," he said.

And those costs continue to rise. According to the Traverse City, Mich.-based research firm the Ponemon Institute, the average cost of a data breach in 2010 was $214 per compromised record, up from $204 per compromised record in 2009.

Doing the math, a data breach that compromises credit card information for just 100 customers could cost a restaurant operator more than $20,000. For a mom-and-pop shop, that cost could easily put the restaurant out of business.

Failure to protect stored data

A second pitfall to avoid, Horton said, and one of the top reasons a merchant is most likely to fail a PCI audit, is the failure to adequately protect stored data.

"VeriSign Global Security Consulting Services, a division of security services vendor VeriSign, has conducted hundreds of PCI assessments in recent years," he said. "Of the merchant companies assessed by VeriSign, 79 percent were cited for the failure to protect stored data and thus failed their assessments."

Compliance doesn't equal security

A third pitfall to avoid when it comes to PCI compliance is thinking that compliance equals security. That's just not the case, experts say.

"Just because you are compliant or validated doesn't mean that you are secure," said Steve Elefant, chief information officer of Princeton, N.J.-based Heartland Payment Systems. "And unfortunately you're only compliant until you have an issue and then you are no longer compliant."

"Of the merchant companies assessed by VeriSign, 79 percent were cited for the failure to protect stored data and thus failed their assessments."

— Tim Horton, vice president of merchant product development, First Data

Validated software doesn't make a restaurant compliant

By Brad Cyprus, senior security architect, Vendor Safe Technologies

A common misconception among restaurant operators is that because their software is PCI compliant, the operator is compliant as well. This is a fallacy, and a merchant who makes this erroneous conclusion could be open to any number of vulnerabilities which by themselves would negate the possibility of PCI compliance.

When describing the requirements for Visa's Payment Application Best Practices, a Visa-specific standard that was replaced by the Payment Application Data Security (PA DSS) Standard in 2009, Visa states that, "Visa prohibits the retention of full magnetic-stripe ('track') data, Card Verification Value 2 ('CVV2') and PIN blocks — all critical impediments to achieving PCI DSS compliance."

This shows Visa's own acknowledgement that secure software is required to support PCI, but it is not sufficient by itself. Using secure applications is only a part of the PCI picture.

A failure to meet the other components will result in opening the merchant up to the liability associated with noncompliance. A source for the confusion may be the credit card processors themselves as they ask their merchants the following questions:

- Are you PCI compliant?
- What is the software you are using (manufacturer and version)?

It is possible that the nature of this inquiry has lead merchants to believe that if their software is on the PA DSS list of approved software, they will be compliant. It is important to understand why the processors ask these two questions because while they are related, they are designed to protect the processor and not the merchant.

Credit card processors are interested in protecting themselves from liability. By asking a merchant the question "are you PCI compliant," the processor verifies that the merchant claims to have already taken the necessary steps to protect his environment.

This puts the burden on the merchant to maintain the proper level of security, and it limits the processor's exposure in the event of a breach. A merchant who answers "no" to this question will be prohibited from taking credit cards, even though processors in many instances are not validating an affirmative response.

Furthermore, the processor asks, "What is the software you are using?" This verifies that the software communicates to the processor safely. Software that is on the PA DSS will transmit credit card data securely, further mitigating

the processor's risk. In other words, the processor has taken care of its interests here, but the merchant has not unless he can truthfully claim that he is PCI compliant.

What merchants must understand is that processors want to pass the liability of credit card and identity theft to the merchant, and these questions open the way for processors to accomplish their goals.

There is no doubt that using a PA DSS-approved software is a crucial component of PCI DSS, but if network security also is not implemented properly, then the application will be vulnerable to hackers and other security breaches. In the modern world where identity and credit card theft are becoming more pervasive every day, it is no longer acceptable for locations to ignore potential issues associated with credit card processing.

Merchants looking to protect themselves and their customers will make sure that security is a priority when planning their credit card environment.

Source: Vendor Safe Technologies

Failing to make an adequate investment

Becoming PCI compliant may mean incurring new costs, but finding the right resources and technology can greatly reduce incurring unnecessary costs. By following a few key principles, operators can simplify compliance and empower their business with an active, pragmatic security approach.

Acting alone

Businesses are not expected to act alone, nor should they. In fact, all parties involved in processing card transactions have an imperative to continually improve their data security techniques. Businesses need to talk to the acquiring bank or a knowledgeable business payments advisor. These companies may have resources available to help achieve and maintain compliance.

Rising costs

The cost of data breaches continues to rise.

Average cost of a data breach in 2009	$204 per comprised record
Average cost of a data breach in 2010	$214 per comprised record

Source: Ponemon Institute

Choosing a data security solution poorly

Businesses need to weigh their technology decisions carefully. They should look for flexible, technology-agnostic solutions — ones that work with a system regardless of the POS hardware, card association or processing relationship — and solutions that effectively remove data from an environment while allowing access when needed.

Having a short-term outlook

Businesses need to make a long-term commitment and should develop a thorough, proactive compliance strategy to protect their future. Protecting customer card data requires an ongoing effort.

Chapter 4 Developing a culture of security

Although business operators complete the Self-Assessment Questionnaire on an annual basis, maintaining payment card security is an around-the-clock effort, said Vendor Safe Technologies' Cyprus.

Protecting customer card data requires an ongoing effort. Businesses need to make a long-term commitment and should develop a thorough, proactive compliance strategy to protect their future and take advantage of all available tools.

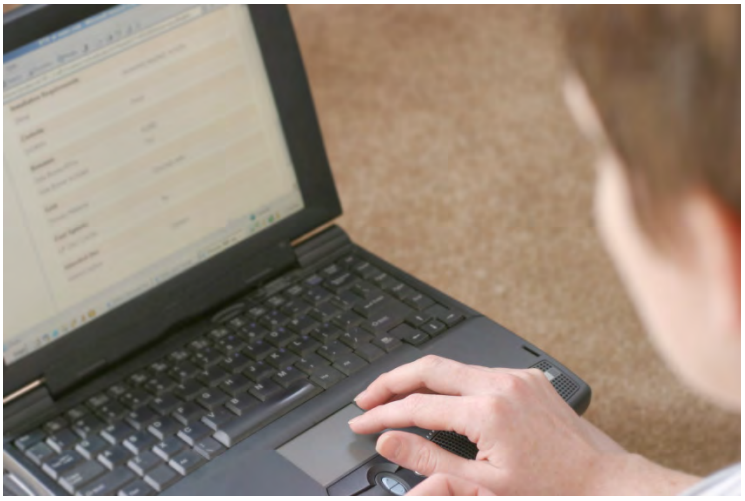
Planning efforts should include ongoing self-audits, efforts to reduce cardholder data environments and other best practice advice as provided by the PCI Security Standards Council.

Cyprus offered a number of best practices that businesses can engage in to help maintain a culture of security.

Keep remote access secure

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 log-in to a server, or it initiates a session which in essence emulates direct access to the remote computer's keyboard and mouse," Cyprus said. "Inevitably, when a credit card breach story makes the news, unauthorized remote access was part of the issue."



When remote access to a network is enabled, it is important to comply with the specific PCI requirements addressing how to keep the network secured.

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.

Requirements 1.2 and 1.3 of the PCI standard prohibit untrusted networks or unnecessary communication to the cardholder environment. The purpose of these regulations 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 user name and password. Without the second factor, if that information was ever compromised, someone else could use those credentials to log in. The second factor ensures that someone accessing the network is actually who they claim to be.

The second factor cannot be more information that a user knows. Instead, 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.

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.

Keep wireless networks secure

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 the 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. 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

Strategies to keep wireless networks secure

- Encrypt data
- Protect the key
- Use a firewall to separate the network from the cardholder data environment
- Install a wireless detection process

business perspective, such as faster order entry and table side credit card processing. 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," Cyprus said.

Maintain robust firewalls

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 also can help prevent 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.

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 more than 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," Cyprus said. "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."

Restaurant operators 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.

Keep software up to date

When PCI was introduced in 2004, 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.

Once compliant software is available, it is up to the merchants to upgrade their systems accordingly. If a location has unsecure 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

Once compliant software is available, it is up to the merchants to upgrade their systems accordingly.

available about credit card breaches, many merchants have elected to ignore the threat and continue running their stores with unsecure 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.

Visa has taken an active role in mitigating this issue by demanding that credit card acquirers, the entities that issue credit card merchant accounts, refuse to accept payments from merchants who are not running PCI-compliant software.

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 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.

Educate 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 and 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," Cyprus said. "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 many ways that merchants can educate their staff. Regardless of how an organization chooses to manage training, it needs to be an ongoing initiative so that there are no holes in an otherwise sound environment.

Employees have the most access to the physical credit cards of customers. To ensure security, it's important to provide credit card security policy updates to staff annually.

Chapter 5 Where to turn for help

Achieving PCI compliance is a lengthy process and one that can be expensive to accomplish. What makes it more difficult for restaurant operators is that they typically don't have an IT staff to help with the process.

The result can be that when an operator fills out the self-assessment questionnaire, it may or may not be completely accurate.

"An operator who is familiar with their technological implementation can go through the assessment, and if there are any questions about which they are unsure, that's when they should talk to an IT security person to make sure they understand what they are answering," PAR Technologies' Kantor said.

"To say they are doing something when in fact they aren't sure is not a good idea," he said. "I've met many operators whose expertise isn't in technology, so in those cases I wouldn't recommend that they attempt to do this on their own."

Although there are a number of resources in the marketplace to help businesses with PCI compliance, the challenge is finding the appropriate one.

The world of PCI compliance has spawned a whole new market for qualified security assessors and it has become a big business. There are hundreds of consultants looking to make a dollar helping business operators get through the process, but the value of those services may not be consistent from one consultant to the next, and choosing the wrong consultant could be costly should a data breach occur.

A number of restaurant operators have chosen Vendor Safe Technologies to assist them with achieving PCI compliance.

Vendor Safe has developed, deployed and supported innovative security technologies for more than 20 years. The company's Network Detecting Firewall Architecture and Global Security Mesh/VPN enables PCI credit card merchants to quickly become PCI compliant at the lowest total cost of deployment and lowest total cost of ownership.

In addition, the company backs its services with a $100,000 guarantee against data breaches.

American Dairy Queen Corp., which operates more than 5,000 locations in North America, partnered with Vendor Safe in August 2010. Through the alliance, Vendor Safe will support ADQ's initiative to help franchisees secure their payment card processing systems, keeping customers' card data and personal

If credit card information is stolen and the merchant has incorrectly filled out the SAQ, the business owner could be held liable and, in fact, could go out of business.

Case study: Fast food franchise security breach (multiple locations)

By Brad Cyprus, SSCP, senior security architect, Vendor Safe Technologies

Company profile

- The business is a franchisee of a national hamburger chain in the southern United States.
- As of August 2008, the franchisee operated eight locations.
- Its POS system is a sophisticated application that allows for centralized management, financial and operational reporting as well as high-speed Internet credit card processing.
- As a convenience to its customers, the company provided an Internet hotspot, which shared the high-speed connection used by the POS system.

Business situation

The franchisee relied on the POS software reseller to be its de facto IT department. The reseller performed a standard installation of the POS software and associated hardware at each location. At some point, the environment was breached and malware was installed on the network. As a result, at least two of the eight locations had credit card data electronically stolen from the system.

Further analysis of the system uncovered that the shared Wi-Fi hotspots were not properly segregated, so direct access to the servers that processed credit cards was possible. It is likely that the Wi-Fi network played a role in the compromise of customer data by being a port of entry for the discovered malware.

The franchisee was notified by VISA USA Inc. and the U.S. Secret Service of the credit card theft and a technical security audit was required to validate the security and business practices at the compromised locations. The results of these audits and the extent of the thefts would determine what types of fines and future requirements the business owner would face, assuming the franchise would be permitted to continue to accept credit cards at all.

The franchise owner realized that the future of his business in part rested on how the security of the locations was improved. To become compliant, the franchise owner sought outside assistance to quickly achieve PCI DSS compliance.

The primary goal of the franchise owner was to protect his network in such a way that he could operate his business while still satisfying the requirements of PCI DSS. The franchise owner also wanted to alleviate a technical issue associated with broadband failure. In the event any of the locations suffered an Internet outage, credit card authorizations could not be processed in real time. In those cases, the system would store the credit card data and hold it until Internet communication was restored. If a credit card processed in that fashion was declined, the business would lose the money associated with that charge.

Results

The franchise owner purchased a solution from Vendor Safe Technologies and had it installed at every location in less than two weeks. By using this managed solution, the franchise owner reduced the effort required to become PCI DSS compliant.

Since the system was deployed, several unauthorized remote access attempts have been blocked and internal threats have been thwarted. The system reports errors in real time, and the Vendor Safe staff monitors traffic to help prevent further credit card issues.

In addition, when broadband failures occur, the monitoring center records the outage while automatically restoring Internet communication using a dial-up connection. Vendor Safe then works with the company's Internet provider to remedy the communication issue.

The Vendor Safe solution solved both the security and business process issues experienced by this customer.

information safe from hackers, thieves and other potential threats using Vendor Safe's PCI Managed Security Suite.

Vendor Safe also will enable franchise owners to easily validate PCI DSS compliance to their acquiring banks.

And POS system provider Squirrel Systems, based in Burnaby, British Columbia, has named Vendor Safe as a recommended solution provider to assist Squirrel customers in achieving PCI DSS compliance through a simplified, low-cost set of tools.

"Merchants in the hospitality industry rely on Squirrel for stable, secure and innovative POS solutions, including payment applications validated to the latest standard, PA DSS," said Bob Mackett, president of Squirrel Systems.

"However, our customers' POS system is only one component of their overall PCI requirements," Mackett said. "The process of becoming PCI compliant can often be confusing and complicated, but we are committed to assisting our clients find the best tools and services to help them reach and maintain compliance. That is why we have carefully selected Vendor Safe for their innovative and proven PCI compliance solutions, which will expand the services that we are able to deliver to our clients and provide them with the peace of mind to focus on running their businesses."

Chapter 6 Terms to know

PCI compliance comes with its own set of often-confusing terms. Here is a short list to help business operators navigate the verbiage.

Account data: Cardholder data plus sensitive authentication data.

Acquirer: Also referred to as "acquiring bank" or "acquiring financial institution." Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.

Adware: Type of malicious software that, when installed, forces a computer to automatically display or download advertisements.

Anti-virus: Program or software capable of detecting, removing and protecting against various forms of malicious software (also called "malware"), including viruses, worms, Trojans or Trojan horses, spyware, adware and rootkits.

Application: Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, Web) applications.

Audit log: Also referred to as "audit trail." Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review and examination of sequence of environments and activities surrounding or leading to operation, procedure or event in a transaction from inception to final results.

ASV: Acronym for "approved scanning vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.

Authentication: Process of verifying the identity of an individual, device or process. Authentication typically occurs through the use of one or more authentication factors such as:

- Something that is known, such as a password or passphrase
- Something that is owned, such as a token device or smart card
- Something the user is, such as a finger print or retinal scan

Authentication credentials: Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device or process

Cardholder data: At a minimum, cardholder data consists of the full primary account number. Cardholder data also may appear in the form of the full PAN plus cardholder name, expiration date and/or service code.

Card verification code or value: Also known as card validation code or value, or card security code. Refers to either magnetic-stripe data or printed security features.

Default password: Password on system administration, user or service accounts predefined in a system, application or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.

DSS: Acronym for "data security standard" and also referred to as "PCI DSS."

Encryption: Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

File integrity monitoring: Technique or technology under which certain files or logs are monitored to detect if they are modified. When critical files or logs are modified, alerts should be sent to appropriate security personnel.

File-level encryption: Technique or technology (either software or hardware) for encrypting the full contents of specific files.

Firewall: Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.

Forensics: Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.

Host: Main computer hardware on which computer software is resident.

HTTP: Acronym for "hypertext transfer protocol." Open Internet protocol to transfer or convey information on the World Wide Web.

HTTPS: Acronym for "hypertext transfer protocol over secure socket layer." Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as Web-based log-ins. ID identifier for a particular user or application.

IDS: Acronym for "intrusion detection system." Software or hardware used to identify and alert operators about network or system intrusion attempts. Composed of sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses a system of rules to generate alerts in response to security events detected.

IP address: Also referred to as "Internet protocol address." Numeric code that uniquely identifies a particular computer on the Internet.

IP address spoofing: Attack technique used by a malicious individual to gain unauthorized access to computers. The malicious individual sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host.

ISO: Better known as "international organization for standardization." Nongovernmental organization consisting of a network of the national standards institutes of more than 150 countries, with

one member per country and a central secretariat in Geneva, Switzerland, that coordinates the system.

Issuer: Entity that issues payment cards or performs, facilitates or supports issuing services, including but not limited to issuing banks and issuing processors. Also referred to as "issuing bank" or "issuing financial institution."

Key: In cryptography, a key is a value that determines the output of an encryption algorithm when transforming plain text to ciphertext. The length of the key generally determines how difficult it will be to decrypt the ciphertext in a given message.

Magnetic-stripe data: Also referred to as "track data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions.

Malicious software/malware: Software designed to infiltrate or damage a computer system without the owner's knowledge or consent. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware and rootkits.

Masking: In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed.

Merchant: For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover Financial Services, JCB International, MasterCard Worldwide or Visa Inc.) as payment for goods and/or services.

Network: Two or more computers connected together via physical or wireless means.

Network components: These include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances and other security appliances.

Network security scan: Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services and devices that could be used by malicious individuals.

Network operating system/OS: Software of a computer system that is responsible for the management and coordination of all activities and the sharing of computer resources. Examples of operating systems include Microsoft Windows, Mac OS, Linux and Unix.

PAN: Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Password/passphrase: A string of

characters that serve as an authenticator of the user.

Patch: Update to existing software to add functionality or to correct a defect.

Payment application: Any application that stores, processes or transmits cardholder data as part of authorization or settlement.

Payment cards: For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC: American Express, Discover Financial Services, JCB International, MasterCard Worldwide or Visa Inc.

PCI: Acronym for "Payment Card Industry."

Penetration test: Penetration tests attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the network trying to come in (external testing) and from inside the network.

Personally identifiable information: Information that can be utilized to identify an individual including but not limited to name, address, Social Security Number, phone number, etc.

PIN: Acronym for "personal identification number." Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for ATMs for cash advance transactions. Another type of PIN is one used in EMV chip cards, where the PIN replaces the cardholder's signature.

POS: Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.

Protocol: Agreed-upon method of communication used within networks. Specification describing rules and procedures that computer products should follow to perform activities on a network.

PTS: Acronym for "PIN Transaction Security." PTS is a set of modular evaluation requirements managed by the PCI Security Standards Council for PIN acceptance.

Public network: Network established and operated by a telecommunications provider, for the specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified and/or diverted while in transit. Examples of public networks in the scope of PCI DSS include, but are not limited to, the Internet, wireless and mobile technologies.

PVV: Acronym for "PIN verification value." Discretionary value encoded in the magnetic stripe of a payment card.

QSA: Acronym for "qualified security assessor." A company approved by the PCI SSC to conduct PCI DSS on-site assessments.

Remote access: Access to computer

networks from a remote location, typically originating from outside the network. An example of technology for remote access is VPN.

Report on compliance: Also referred to as "ROC." Report containing details documenting an entity's compliance status with the PCI DSS.

Report on validation: Also referred to as "ROV." Report containing details documenting a payment application's compliance with the PCI PA DSS.

Re-keying: Process of changing cryptographic keys. Periodic re-keying limits the amount of data encrypted by a single key.

Risk analysis/risk assessment: Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.

Rootkit: Type of malicious software that, when installed without authorization, is able to conceal its presence and gain administrative control of a computer system.

Router: Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.

Security protocols: Network communications protocols designed to secure the transmission of data. Examples of security protocols include, but are not limited to, SSL/TLS, IPSEC and SSH.

SAQ: Acronym for "self-assessment questionnaire." Tool used by any entity to validate its own compliance with the PCI DSS.

Smart card: Also referred to as "chip card" or "IC card (integrated circuit card)." A type of payment card that has integrated circuits embedded within. The circuits, also referred to as the "chip," contain payment card data including, but not limited to, data equivalent to the magnetic-stripe data.

Spyware: Type of malicious software that when installed, intercepts or takes partial control of the user's computer without the user's consent.

SSL: Acronym for "secure sockets layer." Established industry standard that encrypts the channel between a Web browser and Web server to ensure the privacy and reliability of data transmitted over this channel.

TDES: Acronym for "triple data encryption standard" and also known as "3DES" or "Triple DES." Block cipher formed from the DES cipher by using it three times.

Trojan: Also referred to as "Trojan horse." A type of malicious software that when installed, allows a user to perform a normal function while the Trojan performs malicious functions to the computer system without the user's knowledge.

Two-factor authentication: Method of authenticating a user whereby two or more factors are verified. These factors include something the user has (such as hardware or a software token), something the user knows (such as a password, passphrase or PIN) or something the user is or does (such as fingerprints or other forms of biometrics).

WAN: Acronym for "wide area network." Computer network covering a large area, often a regional or company-wide computer system.

WEP: Acronym for "wired equivalent privacy." Weak algorithm used to encrypt wireless networks. Several serious weaknesses have been identified by industry experts such that a WEP connection can be cracked with readily available software within minutes.

Wireless access point: Also referred to as "AP." Device that allows wireless communication devices to connect to a wireless network. Usually connected to a wired network, it can relay data between wireless devices and wired devices on the network.

Wireless networks: Network that connects computers without a physical connection to wires.

WLAN: Acronym for "wireless local area network." Local area network that links two or more computers or devices without wires.

WPA/WPA2: Acronym for "Wi-Fi protected access." Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA.

Source: PCI Security Standards Council