CHAPTER 9

Maintaining PCI DSS Compliance for E-commerce Web Sites

CONSUMERS TODAY FREQUENTLY CHOOSE CREDIT CARDS over cash or debit cards to pay for goods and services. Credit cards offer the convenience of buy now, pay later, which many consumers have come to enjoy. In addition, credit cards have become an integral part of online shopping, which in recent years has exploded as a major competitor to traditional retail stores. Credit cards are at the forefront of payment methods for online auction sites and Internet stores. This technology usage requires security measures to protect cardholders' data, that, if misused, could lead to financial problems and personal stress.

Major payment brands formed the Payment Card Industry Security Standards Council to combat lack of security, as well as hackers and misuse of cardholder information. The council has created a list of standards called the Payment Card Industry Data Security Standard (PCI DSS) to help organizations achieve security. This list of requirements contains information to deter hackers from compromising any cardholder data.

This chapter explores how credit card transaction processing occurs and what PCI DSS is. The chapter will explain why PCI DSS compliance is important and how to design and build a Web site with PCI DSS compliance in mind. The chapter highlights what a PCI DSS security assessment entails and what the best practices are to mitigate risks for e-commerce Web sites with PCI DSS compliance.

Chapter 9 Topics

This chapter covers the following topics and concepts:

- What the most common types of credit card transaction processing are
- What the Payment Card Industry Data Security Standard (PCI DSS) is
- How to design and build a Web site with PCI DSS compliance in mind
- What a PCI DSS security assessment entails
- What best practices to mitigate risks for e-commerce Web sites with PCI DSS compliance are

Chapter 9 Goals

When you complete this chapter, you will be able to:

- Understand types of credit card transaction processing
- Define PCI DSS
- Understand why PCI DSS compliance is important
- Design and build a Web site with PCI DSS compliance in mind
- Understand what a PCI DSS Security Assessment entails
- Understand best practices to mitigate risks for e-commerce Web sites with PCI DSS compliance

Credit Card Transaction Processing

Credit card transaction processing has significantly increased the speed and efficiency of consumer spending;

merchants can sell as fast as a customer can purchase. Almost every store, including Internet-based stores, now accepts credit cards.

Many different types of transaction processing occur and each can use different methods. The two most common types of transaction processing are batch processing and real-time processing.

NOTE

Transaction processing in e-commerce means the online store owner possesses a merchant account.

Batch Processing

Batch processing is the handling of several transactions at one time. The consumer is often not present for the processing of the transaction. In batch processing, receipts are often collected over a short time and then sent in as multiple *batches* or sets of information.

PayPal

In today's busy world, many companies have emerged that specialize in credit card transaction processing. These companies make the transaction process easier for merchants and offer additional security to the consumer. One of the largest companies is PayPal.

PayPal was founded in 1998 and acquired by eBay in 2002. PayPal acts as an alternative to credit card transaction processing. Customers using PayPal don't need to have a credit card. PayPal offers additional security for online consumers because a consumer does not share personal information with the other party in a transaction. PayPal has played an essential part in facilitating e-commerce. This company has become an intermediate step that performs the transaction processing for online merchants, auction sites, and other commercial users. In exchange for performing this function for a merchant, PayPal charges a processing fee. The fee depends on the currency, the location where the money is sent, the country of sender, the country of receiver, and other conditions.

Batch processing is used when an enterprise handles a large number of transactions but needs to save resources to handle the processing. Batch processing is much more common in brick-and-mortar stores than in online transactions.

Real-Time Processing

Real-time processing is the most common type of credit card transaction for e-commerce. A consumer's credit card is charged immediately when a purchase is made. In most cases, the product is shipped the day of purchase. Because the Internet runs in real time, real-time processing, which keeps accurate inventory and sales totals, appeals to merchants.

What Is the Payment Card Industry Data Security Standard?

Established in 2004, the **Payment Card Industry Data Security Standard (PCI DSS)** became a set of widely accepted requirements for enhancing payment account data security. The PCI Security Standards Council (PCI SSC) created the PCI DSS. These five payment companies were involved: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The standard has gone through major revisions. Most recent was version 3.0, which was released in 2014, although several individual requirements did not go into effect until summer 2015.

The PCI DSS was created to help organizations that process credit card payments prevent fraud by having increased control over data and its exposure. The PCI DSS requirements apply to all organizations that hold, process, or exchange cardholder information from any of the major payment brands that are members of the PCI Security Standards Council.

The requirements cover management, policy procedure, network architecture, software design, and other

protective measures for handling transaction systems and cardholder data. The PCI Security Standards Council outlined the requirements and organized them under six major areas of concern. PCI SSC calls them the *six principles*. Within those principles exist 12 requirements, each with many details of what is required to maintain a secure cardholder data environment. The principles and requirements are listed in Table 9-1.

You will learn about the principles and requirements in detail in the "Best Practices to Mitigate Risk for E-commerce Web Sites with PCI DSS Compliance" section later in this chapter. In addition, the full set of standards is available to view at *https://www.pcisecuritystandards.org*.

NOTE

Web applications represent only a small portion of the requirements to become PCI DSS compliant.

TABLE 9-1 PCI DSS principles and requirements.

PRINCIPLE	REQUIREMENT
Build and maintain a secure network.	Requirement 1: Install and maintain a firewall configuration to protect cardholder data. Requirement 2: Don't use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data.	Requirement 3: Protect stored cardholder data. Requirement 4: Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program.	Requirement 5: Use and regularly update antivirus software or programs. Requirement 6: Develop and maintain secure systems and applications.
Implement strong access control measures.	Requirement 7: Restrict access to cardholder data by business need to know. Requirement 8: Assign a unique ID to each person with computer access. Requirement 9: Restrict physical access to cardholder data.
Regularly monitor and test networks.	Requirement 10: Track and monitor all access to network resources and cardholder data. Requirement 11: Regularly test security systems and processes.
Maintain an information security policy.	Requirement 12: Maintain a policy that addresses information security for employees and contractors.

If PCI DSS Is Not a Law, Why Do You Need to Be in Compliance?

Although the PCI DSS is not a government regulation, if a merchant is found not to be in compliance, hefty penalties can occur. If unable to meet requirements of PCI DSS specifications, a mid-sized merchant who deals with 1 million to 6 million credit card transactions annually could be fined thousands of dollars. From Visa, fines for a single month could accumulate to $25,000. If compliance still is not followed, payment brands that belong to the PCI Security Standards Council can remove the merchant's ability to make credit card transactions.

Security breaches have resulted in lawsuits directed at merchants and acquiring banks. Banks have initiated these lawsuits because they have issued credit cards to cardholders whose cardholder data was put in jeopardy. The lawsuits seek to recover costs of reissuing credit cards to their customers. In one example, seven merchants instigated a lawsuit against a software development company and one of its retailers over a security breach that resulted in thousands of dollars in expenses. Fines and lawsuits are just the start of fighting noncompliance with PCI DSS.

An example of the consequences of noncompliance with PCI DSS is CardSystems Solutions Inc. in Atlanta. CardSystems Solutions Inc. is a credit card transaction processing company that was hit by hackers, compromising 40 million card numbers. Visa and American Express cut ties with the company after an internal and forensic review revealed that CardSystems Solutions lacked the proper controls to protect sensitive

cardholder information. CardSystems Solutions was stripped of the ability to process Visa and American Express transactions. MasterCard agreed to work with CardSystems Solutions in the short term to improve compliance. The company must prove that it's in full compliance with PCI DSS or risk losing the ability to process MasterCard credit card transactions as well.

Designing and Building Your E-commerce Web Site with PCI DSS in Mind

Designing and building an e-commerce Web site with PCI DSS seems like a daunting task. In reality, it's not as difficult as you might think. The first step is to determine what kind of merchant you will be. This determination assigns you a label in the form of a level number, from 1 to 4. The merchant level governs the types of audits and assessments your organization will participate in.

A level 4 merchant deals with fewer than 20,000 e-commerce transactions per year. A level 3 merchant processes 20,000 to 1 million e-commerce transactions per year. A level 2 merchant processes 1 million to 6 million transactions per year, and a level 1 merchant processes more than 6 million transactions per year. Level 2 through 4 merchants are required to participate in a self-assessment annually and a network scan quarterly; a level 1 merchant is required to undergo an annual onsite audit and network scans quarterly.

The PCI Security Standards Council provides a development framework for merchants to follow when designing and building an e-commerce Web site. The PCI Security Council refers to this framework as a prioritized approach, designed to mitigate the risks associated with storing, processing, and/or transmitting cardholder data.

The aim of the document is to lower the risks to cardholder data by providing details and recommendations for handling cardholder data. The framework provides general guidelines for organizations to follow to achieve PCI compliance. The six goals, or milestones, within this framework are:

- **Remove sensitive authentication and limit data retention**—Keep sensitive data no longer than necessary. This is an important security concept and a best practice, because if a system or application is successfully attacked, the damage is mitigated by not having too much sensitive data. Ensure also that data is disposed in a safe and secure fashion.
- **Protect the perimeter, as well as internal and wireless networks**—Use firewalls, demilitarized zones (DMZs), and other perimeter security mechanisms to protect the network on the perimeter. Additionally, use logical and physical security measures to protect the network hardware including access points.
- **Secure payment card applications**—Use secure protocols and procedures for the processing of cardholder applications and for communications involved in the processing.
- **Monitor and control access to systems**—Monitor, track, and control who can and cannot access servers and systems where cardholder data is stored. Role-based access control, secure protocols, and auditing are all part of controlling access to systems.
- **Protect stored cardholder data**—Take care that cardholder data is stored somewhere and that its location is secure from both internal and external sources. Internal protection may include physical security measures, role-based access controls, and data encryption. External control includes access controls and perimeter security measures.
- **Finalize remaining compliance efforts and ensure all controls are in place**—Ensure that policies, procedures, and processes designed to protect cardholder data are in place. This includes educating end users on policies and procedures and ensuring they are followed.

NOTE

More information and details regarding these recommendations can be found at *https://www.pcisecuritystandards.org/security_standards/documents.php*.

What Does a PCI DSS Security Assessment Entail?

An auditor conducts a PCI DSS security assessment to determine whether a merchant complies with the current

Data Security Standard. A **Qualified Security Assessor (QSA)** is someone trained, licensed, and authorized by the PCI Security Standards Council to conduct a PCI DSS security assessment.

Scope of Assessment

It's helpful for a merchant to know what is examined during a PCI DSS security assessment. Armed with this knowledge, the merchant will know what is taken into account for each audit. The PCI DSS is divided into six major principles with one, two, or three subsections below each major principle. In all, the assessment covers 6 principles and 12 subsections.

According to the PCI Security Standards Council, security requirements apply to all system components. A *system component* is defined as any computer, network, server, or application connected to cardholder data. Network systems that the PCI SSC assesses include:

- Firewalls
- Switches
- Routers
- Wireless access points
- Network appliances
- Other security applications

NOTE

Network Time Protocol (NTP) is one of the original protocols created for the Internet and remains very valuable today. NTP allows systems across various networks to synchronize their internal clocks.

In addition to auditing network systems, servers are included in the assessment. Common server types that have access to cardholder data include:

- Web server
- Database server
- Authentication server
- Mail server
- Proxy server
- Network Time Protocol (NTP) server
- Domain Name Server (DNS) server

These are common server types generally used in business and are typical in a PCI DSS security assessment. Regarding applications, the PCI Security Standards Council refers to all purchased and custom applications, which include internal and external Internet applications. When a third-party provider manages firewalls, routers, databases, or any other computer application, the third-party provider may conduct its own PCI DSS audit or a PCI DSS auditor may do the assessment.

In addition to examining computer systems, several other categories must be assessed to determine if correct security is in operation. These categories include:

- **Wireless**—If wireless technology is used to store, process, or transmit cardholder information, the wireless network will be tested for required security features. The PCI Security Standards Council has agreed that because wireless technology is unable to be well secured, an organization should weigh the benefits and risks before implementing this technology. The PCI SSC advises that an organization should consider whether the technology is fully needed. If so, wireless use should be limited to non-sensitive information.
- **Outsourcing**—Companies that send their information to third-party service providers for storage, processing, or transmission are **outsourcing**. A Report on Compliance must detail the role of each additional third-party service provider. A key point here is that merchants must contractually require that third-party service providers adhere to the PCI DSS if they deal with sensitive cardholder information.
- **Sampling**—Sampling is the process of an auditor selecting representative elements of all the computer

components in a merchant's network and testing them for PCI DSS compliance. The sample must be representative of the whole and reflect accurately the computer systems currently in place.

Instructions and Content for Report on Compliance

QSAs of the PCI DSS in a merchant's organization are required to complete a Report on Compliance (ROC) for that specific merchant. An assessor must follow each payment card brand's reporting format. Furthermore, the assessor must contact each payment card company and determine reporting instructions and requirements. The ROC includes:

- Contact information for the merchant being assessed
- Date report is being formulated
- Description of merchant's organization
- Third-party service providers with shared cardholder information
- Processor relationships
- Whether the merchant is directly connected to a payment card company
- Point-of-sale systems that the merchant uses
- Subsequent entities that require PCI DSS compliance
- Wireless technologies that are linked or connected to the cardholder environment
- Version of the PCI DSS used for the assessment
- Time frame of the assessment
- Focus of the assessment
- Areas excluded from examination
- Description and drawing of network topology and control mechanisms
- Individuals interviewed
- Documentation reviewed
- Hardware and software in use
- Scan of all externally accessible Internet Protocol (IP) addresses
- Template to report the findings of each requirement and sub-requirement

To create a ROC, the QSAs must complete many fields of information and thoroughly examine the merchant's system. At the end of an audit, the merchant receives a Quality Feedback Form to help ensure the QSA retains a high degree of professionalism and quality. The merchant sends the feedback form to the PCI Security Standards Council, where it's reviewed by the Council's Technical Working Group. If a QSA is deemed lacking, the Council will recommend ways the QSA can improve the auditing process. If the QSA's audit methods do not improve, the PCI Security Standards Council will revoke the license of the QSA and remove his or her name from the QSA database available on the Web site.

Detailed PCI DSS Requirements and Security Assessment Procedures

The assessment process is a rigorous one in which every aspect of a merchant's security system is scrutinized and tested. In a security assessment, a merchant needs to know what is required to be PCI DSS compliant and how these aspects are measured.

Security Assessment Marking Procedure

In an audit on PCI DSS compliance, a QSA goes over the six major headings and grades the organization as either "in place" or "not in place." The QSA determines whether the requirement is in place by following assessment procedures outlined by the PCI Security Standards Council. If a requirement is deemed to be "not in place," the auditor determines a target date by which the organization must rectify the requirement. The auditor can also write additional suggestions or comments.

Best Practices to Mitigate Risk for E-commerce Web Sites with PCI DSS Compliance

The PCI DSS requirements may make the task of becoming compliant seem intimidating. Many organizations may be overwhelmed by the extent of the requirements and not fully understand where to start or how to make sure they stay compliant. Many organizations go about PCI DSS compliance as a one-time event of becoming "compliant." To become and stay compliant, organizations should know basic helpful tips:

- **Apply security measures properly**—Create a clean-up rule, enforce limited access, and enable encryption.
- **Simplify**—Reduce excessive firewall rules to make them as simple as possible. Complex firewalls and rules create environments that are difficult to manage, leading to security flaws that can be exploited.
- **Use firewalls**—Firewalls are easy to implement and help screen a lot of inbound and outbound traffic from the cardholder data environment.
- **Document**—Documentation for any policy or system in the organization helps create a rulebook to follow; it also allows a system administrator to see unnecessary rules that can be deleted for more simplicity.
- **Keep going**—PCI DSS is not a checklist. It's an ongoing process that needs to be monitored daily with full commitment, even when an auditor is not in the building. Stay on top of the requirements and tackle problems before they arise.

The SSC has set up the standards and requirements to help merchants create high-security environments. The best place to start is at the first requirement.

Build and Maintain a Secure Network

The first principle of PCI DSS is to build and maintain a secure network. It includes two requirements. To tackle this PCI DSS security requirement and lessen the risk of security compromise, it's easiest to break down the requirements and deal with them one at a time.

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

A *firewall* is a hardware device or software that controls computer traffic in and out of a network. It examines all traffic, allowing friendly traffic and blocking intrusive traffic. A firewall also tracks, monitors, and controls traffic within sensitive areas of an organization's internal network. A firewall can also block users who don't have the correct security permissions. The PCI Security Standards Council deems firewalls an integral part of any computer security system because firewalls deny unknown interactions from entering the cardholder data environment.

The first requirement calls for a merchant to install and maintain a firewall to protect cardholder data. The following list highlights some of the key security requirements identified by the PCI DSS standard and suggested audit procedures for each one:

- **Use a DMZ**—The DMZ is part of perimeter network security in which servers that must be accessible by sources both outside and inside your network are placed outside the firewall. However, the DMZ is not connected directly to either network, and it must always be accessed through the firewall. This means that external users never gain access to the internal network.
- **Maintain network blueprints**—Maintain a current network diagram, including all connections involving transmission of cardholder data. Include any wireless networks the organization uses. This helps track where security holes might be.
- **Block unused ports**—Verify that the firewall configuration includes a documented list of services and ports needed for business operations. Ports and services falling outside this list can be blocked.
- **Streamline protocol use**—A network can use any number of protocols, many enabled by default. Ensure that all protocols in use have a legitimate purpose and are documented.
- **Review firewall configurations**—Network security requirements change. Verifying firewall configuration requires periodic review of the firewall and router rules to ensure they still apply and protect the network.
- **Restrict cardholder database access**—Examine the firewall to verify that there are indeed restrictions between publicly accessible servers and components storing cardholder data.
- **Verify wireless security**—Verify that perimeter firewalls are installed between wireless networks and cardholder data.
- **Hide IP addresses**—Implement IP masks. Hide IP addresses so they will not be translated and revealed on the Internet.
- **Use host-based firewalls**—Ensure that firewalls are installed and correctly configured on mobile systems

such as laptops. Employees should not be able to alter the firewall.

Requirement 2: Don't Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

The second requirement is that merchants not use vendor-supplied defaults for system passwords and other security parameters. Hackers often use vendor-supplied passwords and default settings to gain access and compromise security systems. Vendor-supplied passwords are well known within the hacker community and can be determined easily.

This requirement is fairly simple to comply with. Change passwords and parameters to increase the security level. This list highlights recommendations for passwords and other security parameters:

- **Change passwords**—Change default vendor-supplied passwords on all equipment including routers and access points.
- **Change default wireless configuration**—Change the passwords and default security configurations on all wireless access points (APs). This includes changing the **service set identifier (SSID)** of each AP. An SSID is a unique client identifier sent over a wireless network as a simple password used for authentication between a wireless client and an access point.
- **Develop security standards**—Create configuration standards for all system components. Identify well-known security vulnerabilities and address them in configuration standards.
- **Streamline protocols and services**—Disable all unnecessary unsecure services and protocols.
- **Disable unused elements**—Remove all unnecessary functionality, for example, scripts, drivers, features, subsystems, file systems, and unnecessary Web servers.
- **Use encryption**—Ensure that all passwords are encrypted when stored and in transit. Sending passwords over a network in cleartext makes them vulnerable.

Protect Cardholder Data

The second principle of PCI DSS is to protect cardholder data. The best way for a merchant to comply with this PCI DSS security requirement is, once again, to break it down into smaller requirements.

Requirement 3: Protect Stored Cardholder Data

The third requirement of PCI DSS is to protect stored cardholder data. This is easily done by ensuring all cardholder information is unreadable no matter where it's stored—in portable media, in backup logs, or even on wireless networks. Another simple tip is to ensure that your organization is not storing any more information that is necessary from the magnetic strip. Ensure that full magnetic strip data is never stored anywhere. Never store the card verification code or PIN verification elements. Store as little information as possible.

NOTE

According to the PCI DSS, encryption is an essential component of securing cardholder data. Encryption is essential because if a hacker gains access to sensitive information without the proper cryptographic key, the data is useless. With encryption, data will be unreadable and unusable by anyone without authority to read it.

Some tips for protecting stored cardholder data include:

- **Store only necessary cardholder data**—It's important to store only relevant and legally required cardholder data and destroy the rest. This approach limits the impact should cardholder data be compromised.
- **Develop a cardholder data retention policy**—All organizations with cardholder data should have a retention policy that states how long data is kept and how it will be stored.
- **Develop disposal policies**—Disposal policies highlight how data will be disposed of after it's no longer required. All data should be disposed of so that it cannot be recovered and stolen by a malicious user.
- **Don't store card validation codes**—Code validation numbers are used to verify non-present transactions such as those conducted over the Internet. These are typically three- to four-digit numbers on the back of credit cards. These numbers should not be stored but simply used as a means of authentication.
- **Don't store PINs**—If **personal identification numbers (PINs)** are obtained, they should not be stored or used

in any way other than for authentication.

- **Use encryption**—All cardholder data should be encrypted both in transit and while stored.
- **Restrict access to cardholder data**—Some form of access control, such as role-based access control, should be used to restrict access to cardholder data.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

The fourth requirement under this principle is to encrypt the transmission of cardholder data across open, public networks. For this requirement, a strong, secure encryption strategy is needed. Ensure your organization's decryption software is stored separately. If a hacker does gain access to your data and then encrypts it with a strong encryption key, the data is then rendered useless.

NOTE

Confidential information that is part of the cardholder data environment must be encrypted when being transmitted across any public network. It must be encrypted because public networks are extremely easy for a hacker to access. A hacker can intercept, modify, and divert the transmission of data in progress.

To secure data in transmission, consider the following:

- **Use encryption protocols**—Use strong cryptography and security protocols to protect data when being transmitted over open, public networks. This includes using Hypertext Transfer Protocol Secure (HTTPS) to secure online transactions.
- **Secure wireless communications**—If transactions occur over a wireless link, use secure protocols to secure the transaction. For wireless, these may include **Wi-Fi Protected Access (WPA)** and WPA2. Don't use the Wired Equivalent Privacy (WEP) protocol to secure wireless connections—it's not considered secure.
- **Monitor communications and protocols**—Periodically verify that the most current and up-to-date protocols are being used to secure the communication. Also, ensure that the security protocols are configured correctly. For instance, use a minimum 104-bit encryption key and 24-bit initialization value.

Maintain a Vulnerability Management Program

The third principle under PCI DSS is to maintain a vulnerability management program, and it includes two requirements. Following the strategy used with the last two principles, start by breaking it down into its specific requirements.

Requirement 5: Use and Regularly Update Antivirus Software or Programs

The fifth requirement is to use and regularly update antivirus software. This requirement is quite clear. Whether the user is a typical consumer user, business user, or merchant, up-to-date antivirus software protects a system from malicious attacks, viruses, adware, and spyware.

Three main points to keep in mind about this requirement are:

1. Deploy antivirus software on all systems commonly affected by viruses. Include personal computers and servers.
2. Ensure that antivirus programs are capable of protecting against and, if necessary, detecting and removing other forms of malicious attacks, including spyware and adware.
3. Ensure that all antivirus mechanisms are current, actively running, and capable of generating audit logs.

FYI

Although e-mail offers many advantages in the workplace, the drawbacks include many vulnerabilities and malicious viruses that enter the network via employees' e-mail. Antivirus software must be used on all systems commonly affected by viruses to protect systems from malicious software. To be effective, anti-malware must be monitored and updated frequently to be sure it's able to respond to the latest threats.

Requirement 6: Develop and Maintain Secure Systems and Applications

The sixth requirement under PCI DSS is to develop and maintain secure systems and applications. Hackers often gain access to networks through security vulnerabilities. Often security vulnerabilities in programs and software are addressed by the vendor, and they provide security patches to correct these inconsistencies. Continuous updates and regular maintenance of systems and applications can stop hackers in their tracks. By applying the latest patches and updates immediately, an organization maintains the security of its system by fixing flaws within software programs. This prevents employees, hackers, and viruses from exploiting program and software flaws. Appropriate patches must be tested and evaluated to determine if they sufficiently fix security vulnerabilities.

A few tips on maintaining application security include:

WARNING

Remember, attacks can come from other sources besides hackers. Employees and viruses can be the cause of internal malicious activity within your network. You should consider insufficient training, human error, and intentional circumvention of controls as possibly introducing vulnerabilities.

- **Keep patches up to date**—Ensure all system components have the most recently released vendor-supplied patches installed. Patches should be installed soon after the release date. In a business environment it is important to first test all patches and service packs in a test system before applying to a production system.
- **Develop patching and update policies**—Many organizations choose to develop firm update policies that administrators follow. Systems and applications that are patched and updated are far less likely to be vulnerable.
- **Monitor vigilantly**—Administrators must spend time reviewing and monitoring for the latest threats and vulnerabilities. The monitoring of logs and system errors is often audited in a corporate environment. IT managers who fail to perform and document this kind of monitoring may find themselves subject to discipline by their employers, and may even lose their jobs.
- **Configure automatic updates**—Many systems and applications can be configured to be updated automatically. This takes the human error out of the equation and helps ensure that applications are current.
- **Ensure development follows guidelines**—Develop all Web applications based upon secure coding guidelines. Review custom application code to reveal security threats. Cover prevention of common coding vulnerabilities.

Implement Strong Access Control Measures

The fourth principle of PCI DSS requires organizations to implement strong access control measures. The requirements include enforcing the principle of need to know and enforcing technological and physical access controls.

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

The seventh requirement of PCI DSS is to restrict cardholder data by the business' need to know. This is a requirement companies commonly overlook. Information often flows freely without much care taken to control who knows what within an organization. Many organizations allow employees who have no need to know to access sensitive cardholder data. This becomes a security vulnerability that PCI SSC takes very seriously.

The best way to adhere to this requirement is to initially limit cardholder data to employees whose job functions strictly require this information. All others are restricted. Create a "deny all" feature within the system. This allows the system to keep everyone without authorization from viewing cardholder data.

Some suggestions include:

NOTE

Requirement 7 ensures that sensitive cardholder data is restricted based upon a need-to-know basis. This

means critical information can be accessed only by authorized personnel, creating another layer of security.

- **Enforce role-based access control**—Limit access to cardholder information to those individuals whose job requires such access.
- **Create a "deny all" policy**—Create a method for systems with many users to restrict access based upon users' need to know. The method must be set to "deny all" unless specifically allowed.
- **Develop access policies**—Develop and publish guidelines outlining who can and cannot access specific information. Ensure these policies are reinforced with consequences if a breach occurs.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

The eighth requirement instructs organizations to assign a unique ID to each person with computer access. This requirement seems trivial at first glance. Taking a further look, it's extremely important. If a security breach occurs, user activity must be tracked back to the authorized employee. To comply with this requirement, use passwords, tokens, or biometrics to maintain security. In addition, encrypt all passwords during transmission and storage on *all* system components.

Tips for this requirement include:

- **Develop a two-factor authentication scheme**—A two-factor authentication scheme typically involves combining multiple authentication methods. This may be an ATM card and something only the user knows, such as the card's PIN number. Create a two-factor authentication for remote access to the network for employees, administrators, and third parties. Authentication methods include passwords, biometrics, and access tokens.
- **Require individual access**—Some environments use group access to applications and systems, for example, administrators' groups or guest groups. It's more secure to identify all users with a unique username before allowing individuals access to system components or the cardholder data environment. To increase security, verify that a user has a unique username to access system components and cardholder data.
- **Encrypt passwords**—Encrypt passwords during transmission and storage on all system components.
- **Develop strong password policies**—Password policies may include such items as how often a password must be changed, what characters passwords must include, how long they must be, and how an account is to be locked out after a given number of failed logon attempts.
- **Disable unused accounts**—Accounts for terminated employees should be deactivated immediately and inactive accounts should be disabled after a set period of time.
- **Restrict access**—Ensure that all access to the cardholder data environment is authenticated, including applications, administrators, and other users.

Requirement 9: Restrict Physical Access to the Cardholder Data Environment

The ninth requirement of the PCI DSS states that an organization must restrict physical access to cardholder data. This is a commonly overlooked requirement of PCI DSS. The failure to restrict employees' proximity to cardholder data is a violation of PCI DSS. Organizations must enforce rules on physical access and proximity to the actual credit card data. The organization must also develop a procedure to identify employees and visitors.

Securing physical access is a significant consideration. Some physical security recommendations include:

NOTE

Any physical access to the cardholder data environment will compromise its security. If an individual gains access to the room that houses cardholder data, that individual can remove hard copies or devices. This presents a need for security measures to limit access to the cardholder data area.

- **Restrict physical access to sensitive areas**—Use facility access controls to monitor and limit physical access to systems that store, process, or transmit cardholder data. This may include verifying access control with badge readers, lock and key, or other devices.
- **Monitor the server room**—Use cameras to monitor data sensitive areas. Store camera recordings for at least

three months, unless restricted by law.

- **Restrict access to networking hardware**—Restrict physical access to wireless access points, gateways, hard drives, and handheld devices.
- **Secure backups**—Secure access to backups that may control sensitive data. Many organizations use off-site backup measures as a precaution. Ensure offsite backups are secured during transit.
- **Create visitor policies**—Develop procedures to help personnel easily distinguish between employees and visitors. This is essential in areas where cardholder data is accessible. All visitors must be authorized before entering areas where cardholder data is processed or maintained. All visitors must be given a physical token that indicates they are not employees, and this physical token must expire.
- **Maintain a cardholder paper trail**—Physically secure all paper and electronic media that contain cardholder data. When no longer required, the paper should be disposed of in a secure fashion. This may include using a paper disposal company.
- **Maintain inventories and tracking mechanisms**—Maintain strict control over the storage and accessibility of media that contains cardholder data. Ensure it is known where all sensitive data is stored and how it moves throughout the network, from gathering to storage, backups, and disposal.
- **Dispose of electronic devices appropriately**—Destroy electronic media by purging, demagnetizing, or shredding to eliminate the possibility that the media could be reconstructed. This includes the destruction of hard disks and not just formatting the disk.

Regularly Monitor and Test Networks

The fifth principle of PCI DSS is to regularly monitor and test networks. The two requirements in this principle address network resources, cardholder data, security systems, and security processes.

NOTE

A log's presence in all environments allows tracking and analysis when something does go wrong. If a problem arises and a log is not available, it makes the problem difficult to track and analyze.

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

The tenth requirement of PCI DSS is to track and monitor access to network resources and cardholder data. Logging allows an organization to track all user activity within a system. This helps determine where a problem occurred. The main requirements are to establish a process for linking access to system components to each individual user. Implement automated audit trails for all system components. Secure audit trails so that they cannot be altered, and limit the viewing of audit trails to those with a need to perform a job function.

Some logging best practices include:

- **Develop logging policies**—Logging policies identify what should be logged, how long logs are retained, who has access to logs, and more.
- **Log access to cardholder data**—To track security breaches, it's important to log all individual access to cardholder data. All accounts viewing cardholder data can then be traced.
- **Log failed logon attempts**—To help identify if someone is trying to access cardholder data, log all invalid access attempts.
- **Restrict log access**—Clearly identify who has access to logs and what can be done with that access.
- **Develop retention procedures**—Determine how long logs should be kept and in what form.

Requirement 11: Regularly Test Security Systems and Processes

The eleventh requirement of PCI DSS is to regularly test security systems and processes. Without continual testing of the security systems, hackers can capitalize on systemwide vulnerabilities within processes and custom software. One key feature of this requirement is to conduct quarterly and annual testing of internal and external networks to identify any changes or any new wireless devices, and check for system upgrades.

Regularly testing the security system may include performing penetration testing at least once a year or after any major system infrastructure or application upgrade or modification, and running internal and external

network vulnerability scans.

NOTE

Vulnerabilities are discovered every day by hackers and researchers alike. The vulnerabilities are introduced by new software. Therefore, all systems, processes, and custom software must be tested frequently. This ensures that security is maintained over time, even with any changes that occur within the software.

Maintain an Information Security Policy

The sixth section of the PCI DSS is to maintain an information security policy. This is important because it gives all employees, contractors, and visitors a written management-approved policy. It allows employees to have a guideline for what is the right and wrong use of information. This is considered one of the most basic tools to combat a security breach within an organization.

Requirement 12: Maintain a Policy That Addresses Information Security for Employees and Contractors

This requirement is to maintain a secure, strong policy that allows all employees to understand the security tone that the organization wants to set. It allows employees to know what is expected of them with regard to information security. All employees need to be aware of data sensitivity. It's important for employees to know that data security is everyone's responsibility. Security policy recommendations include:

- **Create and deploy policies**—Establish, publish, maintain, and disseminate a security policy.
- **Update policies**—Develop an annual process to identify new threats and vulnerabilities and include the results in a formal risk assessment. Incorporate this into the security policy.
- **Create usage policies**—Develop usage policies for employee-used technologies. Ensuring that employees are aware of the policy and consequences for not following it.
- **Develop an employee education program**—Implement a formal security awareness program to make all employees aware of the importance of cardholder data security. Educate new employees and current employees not once but as new security developments occur.

CHAPTER SUMMARY

Credit cards are a major part of today's lifestyle. E-commerce activity is a substantial source of revenue for many organizations. The Internet means any organization can become globally accessible. Credit cards enable consumers to purchase from the global market the Internet provides, and this global access brings the need for increased security. Major payment brands formed the Payment Card Industry Security Standards Council to combat lack of security, as well as hackers and misuse of cardholder information. The council has created a list of standards called the Payment Card Industry Data Security Standard (PCI DSS) to help organizations achieve security. This list of requirements contains information to deter hackers from compromising any cardholder data. With PCI DSS compliance, consumers, banks, and merchants can feel secure that their information, clients, and customers will be safe when making purchases.

KEY CONCEPTS AND TERMS

Batch processing
Network Time Protocol (NTP)
Outsourcing
Payment Card Industry Data Security Standard (PCI DSS)
Personal identification number (PIN)
Real-time processing
Service set identifier (SSID)

Qualified Security Assessor (QSA)
Wi-Fi Protected Access (WPA)

CHAPTER 9 ASSESSMENT

1. Because it's a perimeter defense strategy, a firewall is not a critical element of cardholder data security.

   A. True
   B. False

2. You are tasked with designing a security policy for cardholder data. Which of the following are recommended security strategies for cardholder data? (Select three.)

   A. Verify that data is retained for a limited period of time.
   B. Verify that user groups are used to access sensitive data areas.
   C. Verify that data is disposed of properly.
   D. Verify that passwords are encrypted during transmission.

3. Use WEP to secure communications sent over a wired network.

   A. True
   B. False

4. Which of the following elements are typically examined during a PCI DSS Security Assessment? (Select two.)

   A. Firewalls
   B. Network hardware
   C. Employee background
   D. Cached files

5. When credit card transactions are handled in _____, receipts are often collected over a day or week and then sent in as multiple sets of information.

6. PSS DSS is a set of standards designed to help organizations that process credit card payments prevent fraud by having increased control over data and its exposure.

   A. True
   B. False

7. When credit card transactions are handled in _____, a consumer's credit card is charged immediately to complete a purchase.

8. You are attempting to synchronize your Web server to online timekeeping. Which of the following protocols is responsible for managing system time?

   A. TTP
   B. TNP
   C. NTP
   D. CTP

9. Which of the following firewall considerations are recommended by the PCI Security Standards Council? (Select three.)

   A. Use open source firewall systems.
   B. Block unused ports.
   C. Use host-based firewall systems on mobile computers.
   D. Conduct periodic reviews of firewall and router set rules.

10. Merchants should develop a two-factor authentication scheme to protect access to cardholder data.

    A. True
    B. False