CDW PEOPLE WHO GET IT

THE PRINCIPLES OF PCI COMPLIANCE

Take the time to understand and learn to apply the requirements for locking down payment card data.

Executive Summary

Credit card and debit card information are among the most sensitive types of information that organizations must handle. When such data falls into the wrong hands, payment card account number misuse can create identity theft nightmares for individual consumers and financial losses, lawsuits and penalties for the banks and organizations that accept fraudulently presented information.

To mitigate these risks, the card-processing industry developed the Payment Card Industry Data Security Standard (PCI DSS), often referred to simply as the PCI DSS. The standard consists of a detailed set of security requirements that describe methods for storing, processing and transmitting sensitive cardholder information.

Organizations seeking to comply with the PCI DSS for the first time face a daunting challenge. The full PCI DSS contains 75 pages of detailed requirements, along with multiple supplementary documents that provide guidance and requirements for specific technologies and situations.

Fortunately, there are many technology solutions designed specifically to help organizations comply with the PCI DSS. These include firewalls, web application security products, log correlation systems, antivirus packages and more.

TWEET THIS!

Table of Contents

The Situation

Identity theft is an issue of global concern. Thieves regularly attempt to acquire the personal information of individuals to create fraudulent financial accounts and steal funds from existing credit and debit cards.

Many people don't realize that there are multiple victims of these financial crimes, in addition to the individuals who have their identities stolen. Organizations that accept fraudulent credit cards and the banks that process the transactions suffer significant financial and business losses.

The five major payment card brands — Visa, MasterCard, American Express, Discover and JCB — stand to lose the most from these crimes. Although they are not directly responsible for fraudulent transactions, they depend upon the individuals and entities – that bear the financial risk – for their continued survival.

If credit card fraud were to continue unchecked, both consumers and organizations would lose faith in the integrity of the card-processing networks. And they would grow resistant to the higher costs of card processing required to compensate for fraudulent activity. Realizing that they share a common goal of reducing fraud, entities that normally compete in the marketplace came together to form the Payment Card Industry Security Standards Council (PCI SSC).

This organization, funded by the payment card brands and voluntary membership fees, is responsible for creating and maintaining a consistent set of standards that govern the world of payment card processing. The PCI DSS contains strict guidelines governing the ways that organizations handle payment card information, with the aim of reducing payment card fraud.

Contrary to common belief, the PCI DSS is not a law or regulation imposed upon organizations by the government. Rather, it is a voluntary standard that entities agree to follow when they sign a payment card merchant agreement.

These agreements are legally binding contracts: Organizations commit to compliance with the PCI DSS and agree that they will be subject to financial and business penalties if they fail to live up to their compliance commitments. These commitments include implementing the security controls described in the PCI DSS and conducting a series of periodic tests and assessments to validate compliance to the merchant bank that processes their payment card transactions.

The bank, in turn, has a responsibility to the credit card brands to ensure that all organizations using the bank's network adhere to the PCI DSS requirements. Banks and organizations take this responsibility very seriously, as the penalties for failure to comply can run to thousands of dollars and might restrict an organization's future ability to participate in the payment-processing network.

PCI Compliance Defined

The PCI standard sets a threshold for compliance that represents an acceptable level of information security controls surrounding payment card transactions. Organizations that meet the requirements described in the PCI DSS have taken the basic steps necessary to properly secure cardholder data, the ultimate goal of the standard.

It is important to remember that the PCI DSS is mostly a codification of information security best practices that IT professionals have adopted over the years. For this reason, it is often easier to approach PCI compliance when an organization is also adopting a comprehensive approach to data security in general.

The controls required by the PCI DSS include firewalls, encryption, antivirus software, strong passwords and other security measures that are common-sense best practices. Entities already having strong data security programs will find that PCI compliance may require only tweaking the controls in place and adopting documentation, testing and validation procedures.

Who Must Comply

The PCI DSS applies to two types of organizations: those that accept payment cards (typically referred to as merchants) and service providers that facilitate transactions. Merchants must comply based on the terms of their credit-card-processing agreements with their banks.

Service providers must comply because merchants are permitted to conduct business only with PCI-compliant service providers. Essentially, any organization involved in the storage, processing or transmission of credit card information must comply with the PCI DSS.

The PCI SSC developed the PCI standard with input from the payment card brands, merchants and service providers. The council uses a collaborative process to update the standard on a three-year cycle based on feedback from everyone involved in payment card processing. The current version of the standard, PCI DSS 2.0, can be found on the PCI SSC website.

Although organizations must comply with all aspects of the PCI DSS, the payment card brands divide organizations into levels that dictate the types of validation that they must perform to prove their compliance. For example, Visa divides merchants into four levels based upon the number and type of Visa transactions processed annually:

- **Level 1:** Merchants who process more than 6 million transactions annually
- **Level 2:** Merchants who process between 1 million and 6 million transactions annually
- **Level 3:** Merchants who process between 20,000 and 1 million e-commerce transactions annually

- **Level 4:** Merchants who process fewer than 1 million total transactions and fewer than 20,000 e-commerce transactions annually

Visa does not set specific validation requirements for Level 4 organizations, leaving that determination up to the merchant's bank. Level 2 and 3 organizations must complete an annual self-assessment, conduct quarterly network scans and complete an attestation of compliance form. Level 1 replaces the self-assessment with a compliance report by a qualified independent qualified security assessor (QSA).

All of the card brands have similar systems based on annual transactions. MasterCard and Discover use the same four-level system as Visa. American Express has a three-level system with categories of less than 50,000 transactions, 50,000 to 2.5 million transactions, and more than 2.5 million transactions. JCB has a two-level system — more than or less than 1 million transactions.

Hardening POS Systems

A common source of credit card security breaches are the point of sale (POS) systems used to perform credit card transactions. These sophisticated, computerized cash register systems handle all aspects of a customer transaction, including accepting payment via credit or debit card.

POS systems are often networked with other systems that process and store data on a centralized server. In the case of large organizations, the POS system might be linked to a large network of servers and data centers. Consequently, the risk from exposing data through a security breach increases exponentially.

There are three specific vulnerabilities that the IT team should consider when securing a POS system:

- **Remote access:** Allowing employees to remotely manage POS terminals can create openings for attackers to gain access to the system and the sensitive data it handles.
- **End-user devices:** POS terminals are often full-featured systems. They require the same degree of security protection as a desktop computer, for example. Failure to apply security patches, update antimalware software and configure host firewalls can lead to system compromise.
- **Network connections:** The links that connect POS terminals to one another and the server must be secured to prevent attackers from gaining access or eavesdropping on communication. This is particularly critical if wireless networks connect the terminals.

The PCI standard contains controls designed to mitigate risks. For example, properly applying the network security controls described in the PCI DSS should result in a network resistant to eavesdropping and intrusion. Similarly, the host security controls and remote-access provisions can safeguard POS systems against related risks.

5 Benefits of Compliance

Many organizations consider compliance with PCI and other regulations a nuisance imposed upon them by regulators. But it's important to realize that compliance also brings business benefits.

Here are five specific benefits that organizations typically realize as a result of their PCI compliance efforts:

1. Decreased risk of a security breach
2. Peace of mind
3. Avoidance of costly fines
4. Easy path to a secure environment
5. Customer confidence boost

The "Digital Dozen" Requirements

The complete PCI DSS contains 75 pages describing the specific administrative, technical and physical controls required to secure credit and debit card transactions. The specifications fall under 12 requirements, known as the "Digital Dozen," then grouped into six major implementation categories:

1. Build and maintain a secure network.
2. Protect cardholder data.
3. Maintain a vulnerability management program.
4. Implement strong access control measures.
5. Monitor and test networks regularly.
6. Maintain an information security policy.

Build and Maintain a Secure Network

The first set of requirements revolves around network security practices, including the secure configuration of routers and firewalls and the elimination of default passwords.

- **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data.

Any organizations using systems to handle cardholder data must protect those systems with a stateful inspection firewall. It must segment the network into appropriate zones and isolate cardholder systems, both from the Internet and non-cardholder zones of the internal network.

In addition, mobile devices (including any personal devices used by workers) within or to interact with the cardholder data environment must have host firewalls installed and properly configured.

- **Requirement 2:** Do not use products' default passwords or other pre-set security parameters.

It's necessary to change factory-set passwords, Simple Network Management Protocol (SNMP) community strings and wireless encryption keys, before connecting equipment to

the network. Systems must be configured to provide only the minimum necessary services and to require strong security, including the use of encryption for remote administrative access.

Interestingly, the requirements sometimes address items that may not seem directly related to the requirement title. For example, it's a bit unexpected for a requirement that ostensibly covers changing manufacturer-set defaults to also include requirements for disabling unused services and requiring encrypted administrative access to servers. For this reason, it's important that the IT team review all subrequirements in detail when implementing a PCI DSS compliance program.

Protect Cardholder Data

The second category of requirements involves minimizing use of cardholder data and applying appropriate security controls to protect that data, both while it is stored and in transit over the network.

- **Requirement 3:** Protect stored cardholder data.

Organizations should try to reduce the amount of cardholder data that they store and never, under any circumstances, store personal identification numbers, card verification codes or the full contents of magnetic stripes. Strong encryption and key management practices must protect stored payment card numbers.

- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks.

Organizations must use strong cryptography to secure payment card information when it's sent over the Internet, wireless networks and via email or other messaging systems.

The minimization principle is an excellent approach to PCI compliance efforts generally. If the IT team can convince managers to reduce the amount of cardholder data that is processed or stored, as well as the number of system components that touch that information, it will be able to shrink the overall scope of the compliance efforts, thereby helping to facilitate a successful PCI strategy.

Maintain a Vulnerability Management Program

All entities must implement security controls to protect against malicious code and other known vulnerabilities. This includes measures to ensure staying current on emerging threats and taking appropriate action to protect against them.

- **Requirement 5:** Use and regularly update antivirus software or programs.

IT shops must implement antivirus software on all desktop computers, servers and other devices commonly affected by malicious code. Software must be regularly updated with current virus definitions.

- **Requirement 6:** Develop and maintain secure systems and applications.

Systems and software used within a cardholder data environment must receive critical security patches within one month of their release. The IT department must also provide a vulnerability monitoring program, establish change control procedures and use secure coding practices. If the organization has public-facing web applications, those apps must either be protected by a web application firewall or regularly assessed for vulnerabilities.

The requirements in this category may seem innocuous at first glance but contain some of the most detailed controls required by the PCI, especially for public-facing web apps.

Implement Strong Access Control Measures

Access controls are one of the cornerstones of information security, limiting system and information access to individuals with appropriate authorization. There are three requirements in this PCI DSS category.

- **Requirement 7:** Restrict access to cardholder data based on need to know.

Systems and apps must strictly limit access to cardholder information to individuals with a legitimate need to access the information. This must be done using an access control system with a default "deny all" policy.

- **Requirement 8:** Assign a unique ID to each person with computer access.

The IT department needs to create unique login IDs and apply strong authentication measures. Any remote access to the network must require multifactor authentication.

- **Requirement 9:** Restrict physical access to cardholder data.

Entities must establish facility entry controls and use video surveillance to monitor cardholder systems. This requirement also mandates visitor control procedures, inventory processes and the appropriate destruction of electronic media when it is no longer needed.

Organizations that run their own data centers may find that they need to revise their physical security controls after reviewing the detailed specifications in Requirement 9. Those that use outsourced services or colocation sites must ensure that the third-party providers meet the PCI DSS physical security requirements. Typically, these third-party providers undergo their own PCI compliance attestations as service providers.

Monitor and Test Networks Regularly

In addition to implementing the physical, technical and administrative controls described in the previous four categories, organizations must develop routine procedures to ensure that they maintain compliance over time.

- **Requirement 10:** Track and monitor all access to network resources and cardholder data.

The IT team must maintain detailed logs from cardholder system components for at least one year. But either a staff member or an automated tool must review the logs each day. The requirement contains detailed provisions about what must be included in the audit trail.

- **Requirement 11:** Regularly test security systems and processes.

The IT department must conduct quarterly wireless scans, quarterly network vulnerability scans and annual penetration tests. Technical controls must also include the use of intrusion detection systems and file-integrity monitoring tools.

This category includes a number of ongoing activities that must be conducted to maintain compliance. Many IT shops use a checklist approach to ensure that they perform each activity at the required time.

One of the other major compliance challenges that organizations face revolves around log management. This is a critical step in building a solid information security environment and staying ahead of potential attackers, as logs provide important clues that might tip off security staff to intrusions in progress or provide evidence of a suspected breach.

Many entities undertaking a PCI compliance program for the first time find that they don't have a robust event management system and are not maintaining the records needed to meet the provisions of Requirement 10. Log management software can assist with meeting this compliance challenge, offering both log retention and analysis.

Some entities may find they can sidestep the rigors of this requirement if they do not store cardholder data: another strong argument for minimizing the extent to which cardholder data is retained.

Maintain an Information Security Policy

The final category includes a single requirement.

- **Requirement 12:** Maintain a policy that addresses information security for all personnel.

Organizations subject to the PCI DSS must maintain written policies covering a variety of information security activities and review those policies on an annual basis. A specific individual or team must be designated to fulfill the various security responsibilities, conduct security awareness training and perform pre-employment background checks.

Before tackling a compliance initiative, the IT department's members should thoroughly read the standard, which can be found on the PCI SSC website.

Note: It's also important that representatives from the entity, who are knowledgeable about how payment cards are used, are involved. Although PCI DSS requirements often appear IT centric, sometimes the easiest path to success will involve making a simple change to a workflow involving payment card transactions.

A Framework for PCI Compliance Initiatives

Becoming PCI-compliant may have ripple effects throughout an organization. To make the transition as stress-free as possible, consider using this four-step framework:

- **Step 1: Define the scope.** Begin by defining the boundaries of the cardholder data environment. Taking steps to narrow these boundaries as tightly as possible will reduce the effort required to become compliant. Therefore, spending some time on this step is worthwhile.
- **Step 2: Evaluate requirement needs.** Once the scope of the compliance effort has been defined, identify the specific requirements that apply to the organization's operations. For example, if there are no web applications, a web application firewall won't be necessary. One of the best ways to evaluate and define the necessary requirements is to review the various self-assessment questionnaires (SAQs) on the PCI SSC website and identify those that apply.

  For obvious reasons, it is important to determine which SAQ applies to each organization. Guidance about selecting the proper SAQ is also available on the PCI SSC website, and the deciding factors generally revolve around how the organization makes use of payment card data.
- **Step 3: Identify obstacles and set a plan.** Next, perform a gap analysis using the SAQs. Which security controls are already in place? Are there controls that require tweaks to reach compliance? Are major controls missing? Develop a plan to move from the current state to a compliant one.
- **Step 4: Execute the plan.** Finally, begin the work of bringing the organization into compliance. Depending upon the number of transactions processed annually, the entity may need to submit either an SAQ or a third-party report on compliance (ROC) to its merchant bank.

Overcoming Challenges

One of the most significant issues that IT departments must address when working on PCI compliance is a tendency to overlook details in the standard and not abide by the requirements outlined in PCI DSS documents.

Security professionals need to take time to educate both themselves as well as senior management about compliance obligations. From a management perspective, it can help to focus on the implications of noncompliance:

- **Fines:** Banks can levy fines on organizations that fail to comply with the PCI DSS. These may range from small amounts, such as $25 per month, to significant fines in the

tens of thousands of dollars. It's important to understand that organizations need not suffer a breach to receive a fine. Failure to comply with the standard is enough to incur financial penalties.

- **Breach penalties:** If an organization has a breach of cardholder information, then it may be subject to substantial sanctions if it is found to be noncompliant with PCI DSS requirements. Visa, for instance, reserves the right to levy fines up to $500,000 per breach if an organization is breached and found to be noncompliant at the time of the breach. There's also the potential for the organization to be held responsible for all direct costs that result from a breach.
- **Reputational fallout:** In the event that news of noncompliance becomes public, an organization stands to lose face with its customers or constituents, which may affect their willingness to make purchases in the future. There's also the potential for harming the organization's brand reputation generally — not just with current customers or constituents.

It is important to remember that simply holding credit card information creates an environment of potential risk. The best course of action, therefore, is to minimize the amount of such data stored, processed and transmitted, which immediately reduces both the security exposure and the scope of compliance activities required by the PCI DSS.

Taking a Holistic Approach

Beware of taking a passive attitude when it comes to PCI compliance. In the words of one CIO of a global retailer, "PCI feels like something that is being done to me and not something being done with me."

Organizations that have the most successful compliance programs eschew this attitude. Instead, they adopt an active approach to compliance.

Instead of designing to the standard, they focus their efforts beyond just protecting credit card information. These IT teams craft security programs that encompass all elements of protecting their networks, systems and data from abuse or misuse.

The Policy Component

Policies form the core of any well-designed information security program. They both designate information security responsibilities and provide staff with the appropriate authority to implement controls. Therefore, organizations seeking to become PCI-compliant may wish to start by creating a set of information security policies that meet the specifications of PCI DSS Requirement 12 and outline the organization's overall approach to information security.

Policy development should include a review of each of the major elements of security:

- **Data security:** testing, identity and access management, antivirus software and password security requirements
- **Network security:** firewall and network device management, remote-access provisions and encryption standards
- **Physical security:** access procedures, inventory mechanisms, visitor controls, video surveillance and data destruction requirements
- **Personnel security:** user education and training, background checks and design of proper workflows to protect cardholder information

IT teams can use this policy framework to build out an appropriate set of information security controls. The IT team can choose to implement a centralized security operations center (SOC) that monitors information security on a 24/7 basis, often with the assistance of specialized security information management software that provides central oversight of security technologies and operations.

While IT departments should always strive to minimize the scope of their PCI-covered activities, the SOC can cover areas beyond compliance scope that may nevertheless be important to the organization.

A comprehensive testing program is another key element of a PCI compliance framework. The overall framework begins with policies that outline the organization's control objectives and continues with tactical controls that implement those policies.

The final element necessary for a well-rounded compliance program is an assessment team that conducts testing to ensure that all technical, physical and administrative controls are correctly deployed and functioning properly. In some instances, such as quarterly external vulnerability scans, IT shops may be required to engage an external party.

In others, such as penetration testing or application security review, organizations may find it impractical to maintain the necessary skills and tools in-house. In this case, they may elect to engage a third party for that reason.

Commonly Overlooked Areas

There are two portions of the PCI standard commonly overlooked or misunderstood by security professionals: virtualization security and log management.

Many IT departments have deployed virtualization to maximize the use of resources and reduce costs. From a compliance perspective, organizations must ensure that they continue to meet the requirements of PCI DSS Section 2.2.1, which mandate that customers implement only one primary function per server.

This requires the implementation of security measures that strongly separate virtual hosts that are in scope from those that are out of scope. Virtualization may also change the ways that the IT team approaches control implementation. For example, Trend Micro and Kaspersky Lab have found ways to

tie antivirus into the hypervisors, eliminating the need to load antivirus on each individual virtual machine.

Organizations migrating to a virtualized environment, or considering doing so, should refer to detailed guidance on the topic issued by the PCI SSC in "PCI DSS Virtualization Guidelines," released in June 2011 and found on the council website.

Log management is a routine task that provides a solid foundation for any information security program. However, it is also one of the most overlooked. Security staff often find log management to be tedious work that doesn't always provide an immediate return on their investment. But well-maintained logs can be crucial during forensic analysis of a known or suspected security incident.

The use of logs can rule out the possibility of cardholder data compromises or confirm an IT team's worst suspicions. Organizations should carefully review PCI DSS Requirement 10 and configure security incident and event management software to meet its requirements.

Another option is to engage a managed service provider to handle the grunt-work of log review. This way only interesting or important events are escalated to the organization's staff.

5 Basic Annual Compliance Assessments

1. Regularly assess internal and external networks for potential vulnerabilities. Use an approved scanning vendor to conduct quarterly external network scans.

2. Perform penetration tests at least once a year. This must be conducted by a penetration testing vendor or a qualified employee, independent from the controls being tested.

3. Conduct a code review of all applications prior to deployment. Any software developed by the organization for use in the cardholder environment must undergo a formal code review process.

4. Assess or protect web applications from common attacks. Unless behind a firewall, web apps must be assessed regularly to ensure they are not vulnerable.

5. Use wireless scanning to protect against rogue devices. The IT staff must conduct quarterly scans to detect the presence of rogue wireless access points on the network.

Organizations may wish to build a compliance calendar to schedule these tests. No IT team wants to find out that it failed to perform a required test.

PCI DSS-related Products

Many vendors offer security products that can help with achieving and maintaining PCI DSS compliance.

Barracuda Networks

The company's line of web application firewalls provides organizations with a PCI DSS compliance solution for public-facing websites that meets Requirement 6.6. These firewalls also protect web apps from direct access to attackers and can add Secure Sockets Layer (SSL) encryption to apps that do not natively support it, helping organizations meet PCI DSS Requirements 3 and 4 as well.

Cisco Systems

The Cisco Compliance Solution for PCI DSS 2.0 implements a strong approach to the security management of networks that contain cardholder data and systems. It follows a three-step process for achieving compliance:

1. Define where sensitive payment information flows and segment those portions of the network.

2. Protect the segmented area with strong perimeter protection, including network firewalls and intrusion detection systems.

3. Provide effective monitoring of the segmented network to watch for threats, misconfiguration and internal espionage.

WatchGuard Technologies

The XTM unified threat management (UTM) product line can help organizations comply with many PCI DSS technical requirements. In addition to meeting the core functional requirements of a firewall, the XTM products provide intrusion prevention, virtual private network (VPN) and gateway malware protection to assist organizations in meeting PCI DSS Requirements 1, 2, 4, 5, 6, 8, 10 and 11.

TIBCO Software

TIBCO's LogLogic log management products facilitate the scalable collection of logs from a wide variety of platforms. LogLogic consolidates these logs and performs high-speed filtering and forwarding to security operations and compliance staff. These products can play an essential role in meeting the provisions of PCI DSS Requirement 10.

Trend Micro

Trend Micro has a variety of security products that can assist organizations in meeting PCI compliance obligations:

- OfficeScan provides malware protection and cloud-based security controls for physical and virtual systems.
- The Endpoint Security Platform offers software distribution, web protection, data loss prevention and patch management services for managed systems.
- Deep Security offers deep packet inspection, firewall services, integrity monitoring, log inspection and patch management for physical, virtual and cloud-based servers.
- Vulnerability Management Services automates the vulnerability scans required by the PCI DSS.
- Email Encryption offers identity-based encryption that protects email messages from eavesdropping without requiring preregistration.

CDW: A PCI DSS Partner That Gets IT

The PCI DSS represents a collection of good security practices. If your organization embraces those requirements for its cardholder data environment, it encourages those practices to bleed over into other areas as well.

As a leading provider of technology solutions for business, government, education and healthcare, we get it. We've helped many organizations navigate the complexities of the PCI DSS and keep payment card information secure.

Your CDW account manager and solution architects are ready to assist with every phase of choosing and leveraging the right security solutions for your PCI compliance needs.

CDW can help with your initial gap analysis, solution design, product acquisition, new technology deployment, encryption, log management and virtualization security. We are also an approved scanning vendor, and can perform your quarterly external vulnerability scans. That same team can address your penetration testing and risk assessment needs as well.

Our data centers offer a range of managed services that can help you tackle tasks such as log and event management or intrusion detection system/intrusion prevention system (IDS/IPS) monitoring. The CDW approach to customer service includes:

- Gap analysis
- Approved scanning vendor (ASV) services
- Wireless security testing
- Internal and external assessment and penetration testing
- Code review
- Secure development training

To learn more about CDW's POS solutions and PCI DSS compliance, contact your CDW account manager, call 800.800.4239 or visit CDW.com/pcicompliance

McAfee An Intel Company

Safeguard critical data and help ensure regulatory compliance with McAfee Data Protection solutions. Available individually or bundled in suites, McAfee Endpoint Encryption and McAfee Data Loss Prevention solutions provide multilayered protection for your data regardless of where it resides — on the network, in storage systems or at the endpoint.

CDW.com/mcafee

Symantec

Symantec's solutions enable you to standardize security, compliance and management across platforms and endpoints, helping to ensure that information, infrastructure and processes can be protected, managed and controlled easily and automatically. Let CDW and Symantec™ ensure that all your data is protected and fully recoverable in the face of any threats.

CDW.com/symantec

TREND MICRO Securing Your Journey to the Cloud

Trend Micro™ Deep Security provides a comprehensive server security platform designed to simplify security operations while accelerating the ROI of virtualization and cloud projects. Tightly integrated modules easily expand the platform to ensure server, application and data security across physical, virtual and cloud servers, as well as virtual desktops.

CDW.com/trendmicro

TWEET THIS!

CDW PEOPLE WHO GET IT