WHITE PAPER

CDW® PEOPLE WHO GET IT™

# PCI DSS COMPLIANCE

A baseline for security best practices, the standard can help organizations improve handling of personally identifiable information.

## Executive Summary

For organizations of all types, every day can bring new challenges. Simply check the headlines. It would not be out of the ordinary to find that another large, multinational enterprise has suffered a cybersecurity attack.

In fact, retail and hospitality companies are among the industries most targeted by hacker attacks, according to Verizon's *2011 Data Breach Investigations Report*, an annual study of security incidents worldwide. Verizon says that point-of-sale (POS) servers and terminals are primary targets for hackers because they often contain valuable customer information.

The Payment Card Industry Data Security Standard (PCI DSS) is a regulatory program created by the payment card industry. Its purpose is to protect cardholder information from exposure because of inadequate security practices by merchants and service providers.

The PCI DSS contains 12 high-level requirements supported by multiple subrequirements. Overall, it offers numerous directives that describe the technical, physical and administrative safeguards that organizations involved in payment card processing must implement.

TWEET THIS!

## Table of Contents

## The Compliance Situation

The aim of PCI DSS compliance is to prevent credit card fraud. Before the release of the first version in 2004, the industry had developed a fragmented approach to reducing fraud, with each card brand creating and managing its own compliance requirements:

- **Visa** – Cardholder Information Security Program
- **MasterCard** – Site Data Protection Program
- **American Express** – Data Security Operating Policy
- **Discover** – Discover Information Security and Compliance
- **JCB** – Data Security Program

Although these programs applied similar principles, merchants were left in the bewildering situation of reconciling the differences and reporting their compliance through as many as five different channels. The PCI DSS consolidated the requirements into a single program and reporting chain, dramatically reducing the complexity for merchants, card brands and financial institutions alike.

The adoption of the standard, combined with a vigorous enforcement program, led to a dramatic increase in compliance during the early years of the program.

Unlike many information security compliance requirements, PCI DSS is not based in law. Rather, it's a contractual requirement placed upon businesses handling payment card information by the payment card industry.

## Behind the Acronym

Organizations facing PCI DSS compliance for the first time are often bewildered by the complexity of the standard and its many detailed requirements. It's important, however, to remember that it is simply a collection of information security best practices, many of which an organization probably already follows.

The standard, developed by the PCI Security Standards Council, contains 12 high-level requirements:

1. Install and maintain a firewall configuration to protect cardholder data.

2. Do not use vendor-supplied defaults for system passwords and other security parameters.

3. Protect stored cardholder data.

4. Encrypt transmission of cardholder data across open, public networks.

5. Use and regularly update antivirus software or programs.

6. Develop and maintain secure systems and applications.

7. Restrict access to cardholder data by business need to know.

8. Assign a unique ID to each person with computer access.

9. Restrict physical access to cardholder data.

10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

12. Maintain a policy that addresses information security for all personnel.

It's difficult to argue with any of these as wise security objectives. As with all security efforts, the devil is in the implementation details. The PCI DSS standard contains 75 pages of detailed requirements specifying exactly how organizations must go about meeting the 12 high-level compliance objectives.

## Challenges and Issues

Failure to comply with the PCI DSS causes a number of complications for organizations. First, there is the direct threat posed by PCI DSS validation requirements. No matter what the compliance level, an organization must provide some sort of validation to the bank that processes its credit card transactions. These validations include:

- Completion of an annual self-assessment questionnaire that provides detailed answers about the controls in place to protect cardholder information. (SAQs are required for all Level 2 and 3 merchants, as well as most Level 4 merchants. See sidebar, *A Leveled Playing Field.*)
- Independent annual audits performed by qualified security assessors (QSAs) or internal auditors for all Level 1 merchants

### A Leveled Playing Field

Although all merchants accepting or processing payment cards must comply with the Payment Card Industry Data Security Standard (PCI DSS), banks require merchants to provide different levels of proof of compliance depending upon the risk their transactions pose. The individual card brands (Visa, MasterCard, American Express and Discover) set these levels, but they all follow the same approach.

For example, Visa sets merchant levels as follows:

- Level 1 merchants process more than 6 million Visa transactions annually.
- Level 2 merchants process between 1 million and 6 million Visa transactions annually.
- Level 3 merchants process between 20,000 and 1 million Visa e-commerce transactions annually.
- Level 4 merchants process fewer than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually.

- Quarterly network vulnerability scans performed by an approved scanning vendor (ASV) for all merchants

If an organization experiences a breach, PCI forensic investigators and auditors will scrutinize its records. If there is any evidence that the enterprise has failed to comply with the standard, it may be subject to significant fines and operational penalties.

Organizations that hold payment card information for any reason — whether they are merchants or simply provide services to merchants — should keep in mind that the mere act of collecting and maintaining credit card information poses risk. In addition to the regulatory concerns raised by the PCI DSS, there are other concerns that should prompt good security practices:

- Although the PCI DSS is not a law, many state data breach notification laws urge organizations to follow the guidelines as laid out for compliance with the standard.
- Organizations also could face civil penalties, including class action lawsuits, from individuals whose personal information has been exposed through a breach.
- Organizations face the loss of reputation and business in the aftermath of a breach.

For all of these reasons, it makes sense to implement strong security controls to stay ahead of individuals trying to steal personally identifiable information. One important, and often overlooked, step in a security and compliance program is the implementation of a robust event management system. These systems help compile, analyze and archive security logs required to monitor network activity and take action in the event of a breach.

## Solution Approach

Organizations that take a holistic approach to security can avoid becoming overwhelmed by approaching PCI DSS compliance actively rather than passively.

The first step is to recognize that there is more to security than just protecting payment card information. It's important to view the PCI DSS as another way to improve the organization's overall security posture.

It is also important to perform a security gap analysis. Completed internally or by an independent third party, the gap analysis can often provide a roadmap offering a route to PCI DSS compliance.

**Virtualization security:** As organizations continue to expand the use of virtualization to improve the efficiency of their data centers, they must also consider the effect on PCI DSS compliance programs. The PCI Security Standards Council has outlined four basic principles that organizations should consider when implementing virtualized environments:

1. The PCI DSS does apply to virtualization technologies.
2. Before adopting virtualization, organizations must consider the risks that the technology introduces.
3. Organizations must study the unique characteristics of their virtualized environments.
4. Specific security controls will vary from environment to environment.

**Log management:** PCI DSS Requirement 10 states that an organization must "track and monitor all access to network resources and cardholder data." The standard goes on to describe in detail the level of tracking required for user and system activity as well as retention requirements for that information.

This boils down to implementing a solid log management strategy. For this, IT shops often turn to security information and event management (SIEM) systems to assist in meeting the log management requirements of the PCI DSS. These systems consolidate records and provide robust analysis and archiving capabilities.

**Building and testing a PCI DSS framework:** The standard requires that an organization incorporate regular testing into its operational approach to compliance. The IT team might want to think of these tests as a way to close the loop on the compliance framework. Staff can begin by creating policies that describe high-level control objectives. These policies must cover a wide variety of topics, including data, network and physical security.

The next step? Design tactical controls that implement and enforce the policies. These controls might include the use of antivirus software, SIEM systems, password management, and other technologies and procedures designed to protect cardholder data.

The final piece of the framework puzzle is testing, which will ensure that the tactical controls function properly. The PCI DSS requires five specific tests:

- Regularly assess internal and external networks for potential vulnerabilities.
- Perform penetration tests at least once a year.
- Conduct a code review of all applications prior to deployment.
- Assess or protect web applications vulnerable to common attacks.
- Use wireless scanning to protect against rogue devices.

It is important to recognize that such tests are in addition to the required QSA audits, self-assessments and ASV scans noted earlier. Although an organization doesn't need to provide the results of its tests to a merchant bank on a proactive basis, it must retain records documenting that the tests took place and that the organization resolved any vulnerabilities discovered.

## 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
- 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**

SONICWALL

Compliance with Payment Card Industry (PCI) data security standards is high on a retailer's list of priorities, especially with recent mandates and high-profile credit card data thefts. Retailers that have not already addressed PCI compliance must do so immediately in order to continue accepting credit and debit card payments. SonicWALL® offers a complete security solution for the PCI environment.

CDW.com/sonicwall

loglogic

TIBCO LogLogic collects and analyzes terabytes of big data generated by IT assets and gives security professionals actionable information to identify issues within their environments proactively for forensics. The primary security value driver is one of mitigating risks: ensuring that security policies are being met and adhered to by user and network activity, mitigating the consequences of potential breaches or noncompliance.

CDW.com

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!

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed.

Together we strive for perfection. ISO 9001:2000 certified

CDW PEOPLE WHO GET IT™