



WHITE PAPER

Understanding & Deploying the PCI Data Security Standard

Understanding and Deploying the PCI Data Security Standard

EXECUTIVE OVERVIEW

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide standard designed to help organizations secure cardholder processing environments. Formed in 2004 by Visa, MasterCard, American Express, Discover, and JCB, in response to the emerging threat to cardholder information, the PCI Standard Security Council (PCI SSC) provides 12 requirements that must be met for compliance with the standard; failure to do so may result in steep fines that can reach hundreds of thousands of dollars. PCI DSS V1.2, the latest update, was released in October 2008; the complete document, as well as what is new with V1.2 can be found at [the PCI Security Standards Council website](#).

The number of records containing sensitive personal information involved in security breaches continues to rise. Cyber-attacks have become more sophisticated, involving not only attacks at both the network layer and the application layer but also other factors such as social manipulation, breakdown in internal security processes and trusted insider abuse. The cost to businesses, in lost revenue and customer loss, can be staggering.

PCI DSS is designed to facilitate global adoption of consistent data security measures to eliminate the loss of cardholder information and clearly defines the steps needed to secure a networked environment. The scope of these requirements is broad but straightforward, giving direction to the service providers and merchants on what technologies, policies and procedures are needed to achieve compliance. PCI DSS incorporates guidelines for perimeter security, data privacy, and application security. This paper outlines these PCI DSS guidelines, and offers recommendations for successfully deploying them.

UNDERSTANDING PCI

The PCI DSS requires any merchant, processor, point-of-sale vendors, financial institutions and payment companies to implement processes, procedures and technology to protect credit card information. There are twelve PCI DSS-required controls that cover access management, network security, incident response, network monitoring and testing and information security policies:

Build and Maintain a Secure Network	<ul style="list-style-type: none"> Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ul style="list-style-type: none"> Protect stored cardholder data Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"> Use and regularly update antivirus software Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ul style="list-style-type: none"> Restrict access to cardholder data by business need-to-know Assign a unique ID to each person with computer access Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ul style="list-style-type: none"> Track and monitor all access to network resources and cardholder data Regularly test security systems and processes
Maintain an Information Security Policy	<ul style="list-style-type: none"> Maintain a policy that addresses information security

According to the standard, all members, merchants, and service providers that store, process, or transmit cardholder data must meet specific security requirements, which necessitate building a secure network and maintaining a vulnerability management program (Table 1). To demonstrate compliance, most merchants and service providers must provide security assessments and perform quarterly network scans to locate and fix vulnerabilities and reduce the risk of intrusion.

Merchant Validation Requirements ¹		
Level/Tier	Merchant Criteria (Annual Transactions)	Validation Requirements
1	Over 6 million	Annual Report on Compliance (ROC) by Qualified Security Assessor (QSA) Quarterly network scan by Approved Scan Vendor (ASV)
2	1 to 6 million (all channels)	Annual Self-Assessment Questionnaire (SAQ) Attestation of Compliance Form
3	20K to 1 million	Annual SAQ Quarterly network scan by ASV Attestation of Compliance Form
4	Less than 20K e-commerce and all other merchants processing up to 1 million	Annual SAQ recommended Quarterly network scan by ASV if applicable Compliance validation requirement set by acquirer

Table 1: Merchant Validation Requirements

DEPLOYING PCI DSS

PCI DSS provides comprehensive direction for the 12 PCI required controls, which can be found in **Payment Card Industry (PCI) – Requirements & Security Assessment Procedures, V1.2**. With many years of experience in the security industry and having assisted many organizations in the deployment of security practices, policies and technologies, Rapid7 has developed additional recommendations to facilitate the process and enhance the success of these compliance initiatives. Starting with a review of best practices for achieving PCI compliance, recommendations are then provided for many of the required controls.

Establish Best Practices

Best practices to effectively secure the cardholder environment and achieve compliance with the PCI standard start with a properly documented, executive management endorsed, information security policy that must be broadly communicated, tested and enforced. These best practices also include understanding the organization’s cardholder data environment (where the data is located and stored and how it moves between applications), regular monitoring of network for potential vulnerabilities, on-going reporting of network activity, and regular inside and third-party penetration testing. *“Best Practices to Protect the Cardholder Environment and Achieve PCI compliance,”* a Rapid7 white paper, provides a review of these best practices.

Deploying PCI and other industry and government standards requires the leadership and/or direction of properly trained information security professionals. The International Information Systems Security Certification Consortium, Inc., or (ISC)², is a non-profit organization based in Florida that provides education and certification for security professionals. The CISSP program and certification provide expertise in ten domains of knowledge that are needed to understand how to implement security procedures. This program covers everything from physical access controls to the law and ethics. It is recommended that at least one person in an organization acquire this accreditation. All Rapid7 consultants are CISSP certified and are trained to assist organizations achieve PCI compliance, from establishing a comprehensive information security policy to testing and validating its effectiveness.

Maintaining a secure network

The first of the 12 requirements in the PCI Data Security Standard is to build and maintain a secure firewall configuration to protect cardholder data. Rapid7 recommends that organizations first “segment” their network into 3 (internal, perimeter, and wireless), and put in place security policies for each:

¹ Visa November 10, 2008 Press Release: “Visa Sets Global DSS Deadlines”

- Internal Security -- Have clearly defined policies in your employee handbook about how your network may be used and what can be attached to it. These are good policies designed to make sure that only authorized devices exist within the internal network. Some examples include:
 - Only authorized machines may access the network.
 - All machines must have their MAC addresses recorded and used in network audits to ensure proper adherence to these rules.
 - All machines must run appropriate anti-virus software.
- Perimeter Security – An unprotected system component on the Internet will be compromised in less than one hour. Maintaining firewall rules on the basis of denying access to everything unless granted is the safest way to stop unintended visitors to your company.
- Intrusion Prevention can block port scans of systems. This is a useful practice since port scanning is a common practice for hackers. IPS Systems are also able to monitor outbound traffic. Trojan horses and worms may connect to their host servers to identify compromised systems that can trigger alarms when traffic stops conforming to established patterns. For example, this can happen when a system makes repeated outbound IP connection attempts to other systems.
- Wireless Security -- There are two categories of wireless devices for which you need to define security policies - access points and clients.

Wireless access points are effective and secure mechanisms for network access when properly managed. We see fewer rogue wireless access point devices as personnel are becoming more aware of the security exposures they allow, but configuration is not easy as there are multiple ways to configure each type. One alternative is to place your wireless access points outside your network and treat all wireless users as insecure remote users even while in the office environment.

Effectively managing the wireless client is a different challenge that is somewhat mitigated by having them appear as external devices to the corporate network. Clients using wireless devices may have their machines compromised while away from the trusted network and should be scanned prior to entry into the network. Companies that have VPN requirements for their wireless users should be additionally cautious. VPN enabled laptops may have been compromised through a non-protected network, such as a home network accessed outside the VPN, which can inadvertently introduce threats into the corporate network upon reconnection.

The second of the 12 requirements in the PCI Data Security Standard involves password protection. Rapid7 recommends that you protect your applications by ensuring that default passwords are changed on network devices, operating systems, databases, test systems, and anything with an IP device address. We like to think that by now everyone changes all their network device passwords on a regular basis but know that they don't. The same passwords get used for many years in some cases. Insiders with that knowledge may be able to access systems years after they've left the employ of the company -- a scheduled program of password changes should be implemented at least quarterly.

Additional protection of applications is achieved through layered access. Establish applications servers behind proxy servers and require access be made through the proxy. Run intrusion detection and firewalls between the internal corporate general access networks and the protected data applications on the inner rings. Establish "calm" networks where all segment traffic is intended for one application and setup automatic performance monitors to detect and report anomalies. The topology of these network segments parallels the "DMZ" concept of isolating servers behind multiple firewalls. Each firewall implements the protection necessary for the relevant segment on which traffic is routed.

The use of layers and protected network topologies is designed to allow the concentration of expenditures and monitoring at the smallest target possible. It makes sense to run intrusion detection and profiling at the application server because the only authorized access has already been allowed into the protected network so an alarm is more serious than if it had occurred on an externally facing IP or other internal network. To get a better understanding of the traffic flowing through your network, use products such as Mazu Networks Profiler. This product uses statistical pattern analysis and NetFlow® data to provide information on internal network traffic and suspicious activity.

Other types of traffic analysis can also be performed on traffic passing through the proxy because an HTTPS port can be decrypted and inspected prior to passing through the router to the application. It is impossible to detect some types of HTTPS attacks because the malware is encrypted inside the data itself.

Protect Cardholder Data

The third and fourth requirements in the PCI Data Security Standard involve protecting cardholder data, including storage of the data as well as encrypted transmission. Data integrity and protection depends upon the needs of the company. While simple in concept, Rapid7 has found that the reality of maintaining data protection and integrity is complex and only reliably done in sophisticated environments.

Policy issues associated with keys and key management, data archiving and retrieval and identity management over time need to be established prior to the implementation of encryption technologies for resting data. Using a combination of encryption and identity management

allows complete tracking of access and content ownership. In all cases, dedicated personnel should be assigned to handle encryption matters including key access and control.

Not having any data at all is the best security you can have. Destroy externally acquired data wherever possible and keep only content for regulatory compliance or customer service.

Customer privacy laws in the United States are weak, mostly being integrated on an ad hoc basis into legislation such as HIPAA. Some states now require notification when personal data may have been compromised, but the handling of the data is undefined. Companies may have their own privacy rules that govern how information that is obtained from individuals is handled, and within Europe, strict controls govern how data of a confidential nature may be handled by commercial enterprises².

Within the PCI environment, there are vendors who sell specialized application solutions that provide end-to-end security for credit card processing.

Maintain a Vulnerability Management Program

The next requirements in the PCI Data Security Standard involve maintaining a vulnerability management program. Internal scanning for vulnerabilities and configuration errors provides the only proof of known vulnerability exposures. Even after scanning, it is still possible that as yet undiscovered vulnerabilities are being used to access systems in an illegal manner.

Email and web sites are the primary entry points for malware. Even the most wary user may accidentally install spyware or other illegal software by visiting an infected or malicious site. We always change the Windows desktop color schemes so that the use of a bogus window masquerading as a dialog box with a "hot" close button can be easily identified. As a result of these continuous attacks, security scanning on a regular basis is required of all machines in a network. Monitoring of devices, ports, services and applications provides a comprehensive view of the network from a vulnerability perspective. There is no point in examining only the application if the underlying operating system or database is insecure.

To minimize the risks of exposure, use the minimum number of different operating systems and patch levels possible. If you can use preset configurations for those systems, it becomes easy to keep up with patching. Microsoft continues to ease the patching of systems with automatic update, which will also help minimize the risk of exposure and provide the simplest patching, configuration, compliance and testing environment possible.

The most effective vulnerability process uses baseline comparison reports. Scanning the established network on a regular (at least weekly) basis and reviewing changes to systems provides trending information, new threat information and information about the differences between the expected and the actual output.

Users often forget to scan test machines which can be some of the most vulnerable. The concept of a "test" machine is that it is not a production machine. Default software installations are often found on these machines which can be compromised easily unless adherent to the corporate security policy.

Rapid7 offers NeXpose, an enterprise vulnerability management product that interrogates devices, databases, applications and web servers. It can be installed as software, an appliance or a managed service solution and performs a comprehensive set of over 20,000 checks against systems.

One area that tends to be overlooked is how to secure custom developed applications, but it is one of the PCI DSS requirements. There are new guidelines to be considered.

Have you modified your application development methodologies to incorporate good security measures?

- Do you have a policy within development that specifies that "bounds checking" is required for all parameter passing?
- Have you assigned a member of the development team as a liaison to the security group?
- Does the security group perform vulnerability testing in concert with development and identify vulnerabilities early in the development cycle while it's easy to change?
- Does your QA department check for possible security vulnerabilities during the QA cycle?

The Open Web Application Security Project at <http://www.owasp.org/index.html> provides help, tools, guidelines and information on how to develop secure web based applications and has many Chapters worldwide that meet on a regular basis. Membership is free.

Weaving security into the development process has taken Microsoft the better part of several long years while being bombarded by an array of attacks that publicized its vulnerabilities to hackers. The huge base of installed software provides an incentive for those with mal intent and it is relatively easy for virus writers to acquire. Yet it is also that very volume of sales that allows the amortization of the costs of the security over so

² http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf



many users. Custom designed applications that get relatively low use are therefore more costly to develop on a per user basis and yet the security needs are the same. This additional cost must be factored into the application budget during planning.

Implement Access Controls

PCI Data Security Standard requires the implementation of strong access control measures. Access controls ensure that critical data is only accessed on an authorized basis. Tracking the usage of access is necessary to provide audit trails so all users must have and use their own IDs. The passwords associated with the IDs must expire on a regular basis but not so fast that users are unable to remember the new ones. We find passwords such as April and May when passwords expire every month! Making passwords expire every 100 days also avoids the quarterly equivalent.

Remember that there are thousands of default passwords established in applications, databases, networking hardware and commercial software. All these need to be found and eliminated. Systems such as NeXpose can perform these password tests through the use of brute force dictionary attacks containing defaults and other commonly used passwords.

Authenticated access is the next protection step above simple password use. The RSA SecurID® product, for example, provides two-factor authentication. Two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator)—providing a much more reliable level of user authentication than reusable passwords. Remote users should be accessing systems only over a VPN with their own certificate keys.

Key management overhead is the cost associated with the personnel who issue, revoke and manage the keys and certificates. The best security model requires that two passwords are needed to access the certificate store. This ensures that two people are required whenever new certificates or keys are generated for additional security but further increases the costs of implementation. The card processing industry does not currently require the use of two-factor authentication although they recommend its use.

Physical access controls should focus on restricting people from getting to the machines that process and store company data. External vendors and internal employees should not be able to access the machine room where processing occurs. Backup media should be encrypted and the keys separately backed up and stored in a different location.

Regularly Monitor and Test Networks

PCI Data Security Standard requires that organizations regularly monitor and test networks and maintain an information security policy. Unfortunately, the trend in most companies is that security becomes important only after a major breach or a new virus runs through the Internet. It is human nature to get complacent about security but that is no longer an option. Security must and will be a part of our daily lives, and implementing a practical policy as the PCI Data Security Standard can go a long way to ensure cardholder data security.

ABOUT NEXPOSE AND RAPID7

NeXpose Unified Vulnerability Management provides continuous, flexible protection from network security threats by accurately scanning Web applications, databases, network devices, operating systems and other software to find threats, assess their risk and create a remediation plan to enable quick resolution. Extensive and flexible reporting shows how certain vulnerabilities can effect an IT environment, helping security professionals prioritize the remediation effort, secure their networks and achieve compliance with government regulations, security configuration policies and the PCI Data Security Standard. NeXpose helps companies implement a measurable and proactive vulnerability management process to ensure a high level of network security without compromise.

Rapid7 is a leader in unified vulnerability management and compliance across an organization's networks, operating systems, databases and web applications. Rapid7 NeXpose is the only solution that includes default support for web applications and manages vulnerabilities for databases. NeXpose separates real threats from massive noise common to most vulnerability management systems, analyzing and sifting through large quantities of data for direct insight into the highest risk vulnerabilities for each business. Companies including Black & Decker, Trader Joe's, Florida State University, the *New York Times*, and the City of Philadelphia rely on Rapid7 to mitigate risk and remain compliant. For more information, visit www.rapid7.com.