

THE SC MAGAZINE WHITE PAPER OF THE DAY – July 1, 2009

Breach Security

The Good, Bad and Necessary: The Complete Guide to PCI 6.6 Success

IT administrators and security professionals are always receiving notification of new rules, regulations and compliance codes that fall under their purview. Just when the necessary adjustments have been made, priorities shifted and new technology purchased, the rules are changed – yet again.

The Payment Card Industry Data Security Standard (PCI DSS) is no different. This resource provides IT security professionals with the information needed to understand PCI compliance and specifically, one of the standard's latest requirements, 6.6.

In addition, the paper offer tips for successful PCI 6.6 compliance and highlights compliance successes from real-world companies.



THE GOOD, BAD AND NECESSARY

THE COMPLETE GUIDE TO
PCI 6.6 SUCCESS

BY: SANJAY MEHTA

JUNE 2009

THE COMPLETE GUIDE TO PCI 6.6 SUCCESS

It seems that IT administrators and security professionals are always receiving notification of new rules, regulations and compliance codes that fall under their purview. And just when the necessary adjustments have been made, priorities shifted and new technology purchased, the rules are changed – yet again.

The Payment Card Industry Data Security Standard (PCI DSS) is no different. The PCI DSS is a requirement of any company or organization that stores, processes, transmits or comes into contact with cardholder data as of June 30, 2005. Most companies with an e-commerce or transactional component to their model fall under this umbrella. This resource provides IT security professionals with the information needed to understand PCI compliance and specifically, one of the standard's latest requirements, 6.6. In addition, the paper offer tips for successful PCI 6.6 compliance and highlights compliance successes from real-world companies.

PCI COMPLIANCE OVERVIEW: WHO ME?

The PCI DSS is the result of a collaboration between Visa and Mastercard to create common industry security requirements. All major credit card companies in the U.S. have endorsed the guidelines of this standard. The 12-point PCI DSS is a requirement of any entity that stores, processes, transmits or comes into contact with cardholder data – period. Nonprofits, government organizations and the private sector alike are all subject to the security standard.

What many organizations don't understand is that PCI compliance provides the necessary – and required – protection of their clients' and partners' credit card information captured and stored online. While the growth and success of online transactions and e-commerce has been critical to the economic growth enjoyed over the last decade, the responsibility surrounding the capture, transmittal, storage, processing and security of the credit card and personal information needed to make that transaction has dramatically increased for businesses. Security breaches have run rampant in both commercial and government environments, which have led to the development of industry standards surrounding the protection of cardholder data.

The PCI Data Security Standard consists for 12 basic requirements:

- **Build and maintain a secure network**
 1. Install and maintain a firewall configuration to protect data
 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect cardholder data**
 3. Protect stored data
 4. Encrypt transmission of cardholder data and sensitive information across public networks
- **Maintain a vulnerability management program**
 5. Use and regularly update anti-virus software
 6. Develop and maintain security systems and applications
- **Implement strong access control measures**
 7. Restrict access to data by business need-to-know
 8. Assign a unique ID to each person with computer access
 9. Restrict physical access to cardholder data
- **Regularly monitor and test networks**
 10. Track and monitor all access to network resources and cardholder data
 11. Regularly test security systems and procedures
- **Maintain an information security policy**
 12. Maintain a policy that address information security

Visa and MasterCard regulations contain more than 200 sub-regulations that organizations must meet as part of the 12 categories listed above. PCI compliance applies to software, infrastructure networks, physical access, business process and documentation. In addition, businesses face the possibility of severe fines and penalties of up to six figures per non-compliance incident. For example, the Visa PCI program maintains that members can be fined up to \$500,000 per incident if any of their Merchant or Service Providers that are not PCI compliant are compromised.

Four merchant validation categories have been outlined:

1. Merchants with more than six million transactions per year (all channels).
2. Merchants with between one million and six million transactions per year (all channels).
3. Merchants with between 20,000 to 150,000 ecommerce transactions per year.
4. Merchants with less than 20,000 ecommerce transactions and who process less than one million transactions (all channels) per year.

All organizations that accept credit or debit cards from the top four major card industry providers – American Express, Discover, MasterCard and Visa – must meet PCI standards. It is not a legal regulation, but rather a contractual obligation with the credit card companies.

PCI 6.6: PROTECTING YOUR APPS

One of the latest requirements facing companies striving to keep up with PCI compliance is requirement 6.6, which is designed to reduce compromises on web-facing applications that result in breaches of cardholder data using a web application firewall, external code review or vulnerability scan. Requirement 6.6 states that all web-facing applications must be protected by having all custom code reviewed for common vulnerabilities by a company that specializes in application security or by installing an application-layer firewall in front of the applications.

Requirements such as 6.6 have been added to the PCI DSS to address the inherently vulnerable nature of web applications. The question used to be whether an organization's web applications would be attacked. The question is now when the attack will occur.

According to Visa Europe's Payment Card Industry Security Scanning Procedures, "Hackers exploit vulnerabilities in these [web application] servers and their scripts to get access to internal databases that could potentially store credit card data...the most elusive vulnerabilities are those introduced through a custom-developed e-commerce application of the merchant or service provider."

Achieving web application security is difficult for most organizations because of the following challenges:

- **Incorporating web application security into the software development lifecycle.** Web application security is a complex field that requires individuals with domain expertise for a successful implementation. Modern web applications use advanced, complicated technologies such as AJAX, web services and Adobe® Flex™, often leaving seasoned development engineers lacking the requisite knowledge to implement security measures during the application design and coding processes.
- **Balancing timely web application updates with the necessary security measures and testing.** Web applications change frequently due to functional updates, content updates and application enhancements. Organizations must constantly balance the business benefits of delivering new functionality in a timely manner with the security team's need to incorporate the appropriate level of security for the web application.
- **Securing interconnected applications resulting from acquisitions, outsourcing or developed by a third party.** Many organizations use applications that were developed by different departments, outsourced to third parties or combined as a result of a merger or acquisition. These applications are often composite applications, developed using different tools, databases and operating systems. In these situations, the connections between the modules may not be secure. In addition, little or no application knowledge may exist in-house to understand or remediate current vulnerabilities.

- **A code review does not remediate any vulnerabilities found.** Conducting a source code review only identifies a web application's deficiencies. The vulnerabilities must then be fixed for the organization to be considered compliant. This is the most common misstep for companies. To fix identified vulnerabilities, a new project must be created to properly update, test and deploy the code changes. Unfortunately, the new project often takes development and quality assurance resources away from other projects and ultimately, impacts the organization's ability to deliver new and often, business-critical releases. With re-evaluation of the code being required after issue remediation is complete, costs can double as well.

Similarly, web vulnerability scanning vendors have recently began promoting the concept that organizations can substitute running their proprietary tools instead of conducting a source code review. These tools require personnel with the proper security skill sets and training to tune, run and analyze the results. Without this knowledge and experience, the thoroughness and effectiveness of the scan is greatly diminished. In addition, scanning tools only look at the web application at a single point in time and do not remediate any issues found.

Web application code review and vulnerability scans are certainly viable pieces of an in-depth web application security approach, despite the above limitations. In terms of PCI DSS Requirement 6.6, however, the benefits of web application firewalls make them a more effective solution for compliance.

THE THIRD OPTION: WEB APPLICATION FIREWALLS

Web application firewalls (WAFs) are the third compliance solution outlined in PCI DSS Requirement 6.6. WAFs overcome the issues associated with secure code reviews and vulnerability scans, and can provide PCI compliance benefits beyond Requirement 6.6.

Web application firewall benefits include:

- **Providing real-time, continuous security for the entire protected application.** A web application firewall monitors the protected web application in real-time, alerts on any security events detected, and prevents attacks and data leakage. The WAF ensures that all components of the application are assessed for security defects, and that the application is continually tested for the latest vulnerabilities, even as new code is deployed.
- **Web application firewalls offer significant cost savings over code reviews and provide an immediate return on investment.** The one-time deployment of a web application firewall can significantly reduce the frequency with which an organization conducts code reviews and vulnerability scans. A WAF should have the ability to dynamically learn and adjust its protection, minimizing additional reviews for each code change. Organizations with multiple or highly dynamic applications can see their web application firewall investment paid back from the cost savings alone.
- **WAFs allow rapid deployment of web application with PCI compliance.** A web application firewall acts as a "dynamic patch" for all its protected web applications, providing security that shields vulnerabilities against exploit. With a WAF, organizations can accelerate their time-to-market while continuing to maintain PCI compliance.
- **WAFs can increase coordination between the security and development teams.** In many organizations, a disconnect exists between the security and development teams. Web applications are often tossed from development into production, providing the security team with little time for review. As a result, the security team may have minimal knowledge of the application it's responsible for protecting.

WEBDEFEND: IMMEDIATE AND CONTINUOUS PCI COMPLIANCE

Breach Security's WebDefend web application firewall appliance offers organizations out-of-the-box PCI compliance. WebDefend not only provides immediate compliance with PCI DSS Requirement 6.6, but also helps companies comply with many other PCI DSS requirements.

WebDefend includes a pre-packaged PCI policy and reports. The PCI policy ensures the proper security configuration for attack prevention and the logging of all payment card use. PCI-specific reports provide an immediate view of the system's overall level of compliance and details of sensitive information use for audit purposes.

WebDefend facilitates compliance with PCI DSS Requirements 2, 3, 4, 5, 6, 8, 10, 11 and 12:

REQUIREMENT	HOW WEBDEFEND HELPS
1. Install and maintain a firewall configuration to protect cardholder data.	Not applicable
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	Blocks known vulnerabilities with signatures developed and updated by Breach Security Labs.
3. Protect stored cardholder data.	Includes a pre-configured PCI policy which blocks all cardholder data from leaking out of web applications.
4. Encrypt transmission of cardholder data across open, public networks.	<p>Ensures SSL strength when sensitive information is legitimately transmitted through web applications.</p> <p>Replicates and decrypts SSL streams – without terminating the original encrypted session. Immediately after decryption, WebDefend fully inspects the traffic entering and leaving the web environment to detect hidden attacks, without compromising performance.</p>
5. Use and regularly update anti-virus software.	Detects web application access by Trojan horses and back-door viruses.
6. Develop and maintain secure systems and applications.	<p>Provides immediate compliance with Requirement 6.6</p> <p>Can act as a "dynamic patch" for application vulnerabilities, including those specifically identified in Requirement 6.5.1 through 6.5.10 of the standard.</p> <p>Learns each protected application and adapts its protection as changes to the application are released.</p> <p>Detects security defects, such as invalid input fields, insecure configuration, weak cryptography, poor session management and others.</p> <p>Detects application changes, enabling secure software development lifecycle (SDLC) management.</p>
7. Restrict access to cardholder data by business need-to-know.	Not applicable.
8. Assign a unique ID to each person with computer access.	Provides user name tracking which analyzes events according to the user who sent the requests and the session ID used. The user name tracking capabilities allow organizations to see suspected and actual attacks from a specific user.
9. Restrict physical access to cardholder data.	Not applicable.

REQUIREMENT	HOW WEBDEFEND HELPS
10. Track and monitor all access to network resources and cardholder data.	Includes four PCI-specific reports: <ul style="list-style-type: none"> • Standard PCI Compliance: Displays brief descriptions of selected types of PCI events. This report focuses on specific types of PCI events and tracks them for a defined period of time. • Detailed PCI Compliance: Displays detailed descriptions of selected types of PCI events. This report focuses on specific types of PCI events and tracks them for a defined period of time. • Credit Card Usage Audit: Provides information on possible payment card leakage events. • Pages in Which Credit Cards Are Displayed: Ties payment card information to specific areas of the web application (web pages, URLs, parameters and others).
11. Regularly test security systems and processes.	Assesses the application passively for defects by monitoring both sides of its communications. WebDefend detects defects, such as invalid input fields, insecure configuration, weak cryptography, poor session management and other insecurities. In addition, WebDefend can detect non-security related application defects.
12. Maintain a policy that addresses information security.	Includes a PCI Standard policy with pre-configured events and responsive actions to ensure protected applications are in compliance with the PCI DSS. Through other rules, enables policy-setting for web application protection across the organization.

Still not sure which route is best to achieving PCI compliance within your organization? Below are examples from real-world companies facing the same decision:

DECISION-MAKING IN THE REAL WORLD



Casual Male Retail Group, Inc., the largest specialty retailer of big and tall men's apparel, maintains over 520 store locations throughout three countries, along with substantial e-commerce and catalog operations. The company is committed to protecting sensitive consumer data and other corporate resources from online application threats, and sought to meet PCI DSS Requirement 6.6

Reviewing its options to comply with the requirement, Casual Male found that the cost of performing code reviews each time application code changed would have been prohibitive. Rather, the company researched WAF devices that could provide immediate PCI compliance, reviewed two leading WAF vendors and decided on WebDefend.

Deployed and running in less than an hour, WebDefend identified the top 10 problem URLs, found automated scanning activity, examples of phishing, leeching and cross-site scripting. The system also discovered application defects, including broken links and infrastructure disclosure.



Overstock.com offers more than 720,000 books, music, movies and interactive games, in addition to more than 100,000 other products online. Committed to protecting customers and their data, Overstock.com chose WebDefend to provide immediate compliance with the latest PCI DSS.

“WebDefend is always protecting us. Overstock.com conducts vulnerability scans daily, but WebDefend is another layer to protect us and our customers,” said Carter Lee, vice president of Information Technology for Overstock.com. “WebDefend’s positive security helps protect Overstock.com from security and compliance issues – as well as the business issues that result from application defects.”

WebDefend provides Overstock.com with real-time, continuous positive security protection, which includes information about vulnerabilities such as a detailed description, location, how it can be fixed and links to additional resources.

HONEYWELL

Honeywell, a \$38 billion diversified technology and manufacturing leader, sought solutions to protect its extensive web layer. The company evaluated several options ranging from assessments and code reviews to web application firewall (WAF) appliances. Honeywell found Breach Security’s WebDefend to be a robust, cost-effective solution. Deployed within hours, one WebDefend sensor was capable of protecting Honeywell’s 5,200 URLs spanning hundreds of web sites as well as the company’s transactional web sites.

The company has achieved significant cost savings by implementing WebDefend. Honeywell previously would have required a team of 10 to 12 personnel to achieve what can now be covered by two employees using WebDefend. As a result, the company is seeing a significant reduction in labor costs.

“Honeywell is saving an estimated \$4-6 million by using WebDefend. We have more than two million types of defects occurring and when you factor in a developer’s cost to fix what WebDefend is able to stop, the savings are in the millions,” said Jim Hinsey, analyst lead security for Honeywell International.



POPCAP GAMES

PopCap Games, the leading multi-platform provider of “casual” computer games, is committed to maintaining the highest data security compliance standards. As PopCap’s web application continuously evolves, PopCap felt that an application review would cost more in the long term, from both the personnel and financial resources, than a web application firewall.

In the end, Breach Security’s WebDefend best met PopCap’s standards for a WAF. PopCap now uses WebDefend to protect its website from application attacks, including detecting sensitive information that may leak.

“WebDefend helps us become aware of the type of attacks that are being directed to our website. In addition, the system also helps us detect any potential application defects,” said Neil Quiogue, information security specialist at PopCap Games International. “The immediate PCI compliance afforded by WebDefend made it an easy sell.”

PEGASUS SOLUTIONS

Pegasus Solutions is the largest third-party marketing and reservation provider in the world, serving the 10 largest U.S.-based travel agencies, eight of the top 10 agencies in the U.K., more than 86,000 hotel properties around the globe, and more than half of the 50 largest hotel companies in the world. Powering hotel reservations for more than 1,000 web sites and services, Pegasus sought a web application security solution to meet a variety of needs, including the PCI DSS Requirement 6.6.

After an extensive review, Pegasus selected WebDefend for its ease of installation and use, out of line deployment capabilities, application defect functionality, and satisfaction of PCI requirements.

“During WebDefend’s initial assessment, the product identified several issues within our environment, including application defects, application design recommendations and potential leakage of sensitive information,” said Michael Jackson, Information Security officer for Pegasus Solutions. “WebDefend was able to not only identify potential problems, but provide granular, detailed information about events within the web application layer to help us quickly and easily remediate issues.”

SEQUOIA RETAIL SYSTEMS

Sequoia Retail Systems, Inc. is the leading independent provider of comprehensive point-of-sale, inventory control, e-commerce and textbook management systems to colleges and universities throughout the U.S.

Hosting e-commerce systems and transactions for its clients, Sequoia needed to meet PCI DSS Requirement 6.6. The company decided to research web application firewalls given the June 30, 2008 deadline, rather than attempt to integrate external code review into its development cycle.

“We selected WebDefend because it provides the best, most comprehensive insight into the behavior of our web applications on a continuous, real-time basis,” said Jeremy Bowers, security manager for Sequoia Retail Systems. “WebDefend goes beyond vulnerability scanning efforts, secure coding initiatives and network security solutions to immediately let us know about approaching threats and specifically alert us to what may be attacking the system. The device serves as a stop-gap measure to prevent threats from affecting our college and university clients, or the cardholder data of their users.”

Sequoia is using WebDefend to protect all e-commerce web sites hosted for its clients. In addition to immediate compliance with PCI Requirement 6.6, the company found WebDefend’s intuitive interface easy to use, and was able to implement and deploy the device in less than a day. WebDefend is able to detect credit card information and mask the data it captures.

INDUSTRY EXPERT OPINION: THE AEGENIS GROUP

Still unsure how to obtain immediate and continuous PCI compliance? The Aegenis Group recently assessed the applicability of the WebDefend application layer firewall appliance within the Payment Card Industry. The Aegenis Group is uniquely qualified to perform this application assessment based on its deep experience in the payments industry and involvement with the PCI DSS. The company’s founders have worked for both Visa Inc. and MasterCard Worldwide, where they participated in the training and continued update of the PCI DSS standard. In 2007, they trained over 7,000 individuals representing over 500 global companies on the PCI DSS standard.

According to the Aegenis Group, “Many companies remain confused about how to achieve compliance with the PCI DSS and specifically, the need for and value of application layer controls. There exists confusion within the industry that network layer scanning, as required by the PCI DSS, is sufficient to both identify application layer vulnerabilities and achieve compliance with the application requirements of the PCI DSS. While network layer scanning is an important component of a comprehensive information security strategy, it doesn’t meet the requirements for application layer security outlined in Requirements 6.5 and 6.6 of the PCI DSS.”

“In addition, the network layer scanning required by the PCI DSS does not accurately detect application layer vulnerabilities such as SQL Injection or Cross-Site Scripting. The unfortunate result is that many well-intentioned companies are exposed to serious risk of data breach because they rely upon network layer scanning to identify application layer vulnerabilities.”

“Breach Security’s WebDefend,” according to the Aegenis Group, “allows companies to address potential application vulnerabilities in a manner that supports and enables PCI DSS compliance and the business objectives of the organization. The primary features that make WebDefend stand out from other WAFs is the ability to deploy the appliance without negatively impacting the network or applications. An additional benefit of the device is its ability to operate out-of-line without introducing any network latency or a single point of failure. Finally, its ability to accurately identify and block sensitive data, while supporting compliance with 23 requirements or sub-requirements of the PCI DSS, make WebDefend a very important component for any comprehensive security program. WebDefend is an elegant solution well-suited to the stringent requirements of the Payment Card Industry.”

ABOUT BREACH SECURITY, INC.

Breach Security, Inc. is the leading provider of real-time, continuous web application integrity, security and compliance that protects sensitive web-based information. Breach Security’s products protect web applications from hacking attacks and data leakage, and ensure applications operate as intended. The company’s products are trusted by thousands of organisations around the world, including leaders in finance, healthcare, ecommerce, travel and government. For more information, please visit www.breach.com.