Observe PCI DSS: How to Audit Application Activity When Logs Don't Help

Dr. Anton Chuvakin

SecurityWarrior LLC http://www.securitywarriorconsulting.com

anton@chuvakin.org

(510) 771-7106

Executive Summary

This paper covers the critical challenges implementing PCI DSS controls and suggests creative solutions for related compliance and security issues. Specifically, the hard problem of security monitoring and log review in cloud, legacy, and custom application environment is discussed in depth. Additionally, clarification of key PCI DSS compensating controls is provided. This paper will help you satisfy the regulatory requirements and improve security of your sensitive and regulated data.

Introduction

If you are like most information technology (IT) professionals, the idea of becoming compliant with PCI DSS or countless other regulations does not sound like an enjoyable task. However, implementing security controls and practices in order to be compliant with PCI DSS or other regulations is a daily reality at thousands of organizations today. In addition, information security and regulatory compliance are related in the minds of many executives as well as IT professionals.

This paper will review some of the challenges implementing PCI DSS controls and suggest some of the creative solutions for compliance and security problems.

PCI DSS Revealed

Visa, MasterCard, American Express, Discover, and JCB banded together to develop PCI DSS to ensure that credit card customer information is adequately protected - and to protect the payment card industry itself. As more and more purchases and transactions are done with credit and debit cards, the importance of protecting cardholder information as well as electronic transactions integrity can only grow. Visa alone does $5.2 trillion dollars in payment card transaction every year, which exceeds the individual GDP volumes of all, but four countries on the planet.

PCI compliance presents a significant challenge to large, distributed businesses. While getting compliant is easier than staying in compliance, even that initial assessment often takes months of work and thousands of dollars in products and services, as well in internal policy changes. Legacy applications as well as newer virtual and even cloud based applications, falling under PCI mandate, present additional challenges.

On the other end of the spectrum, smaller, less security aware organizations face their own dramatic PCI challenges, related to costly ongoing controls, such as log monitoring, as well as controls requiring extensive security knowledge, such as secure application development. Event with simpler security controls such as avoiding default passwords and configuring firewalls, smaller organizations have trouble protecting their data. The recent Verizon Data Breach Investigations 2011 report, for example, still names password guessing as a key risk to card data: '"exploitation of default or guessable credentials" is represented in two-thirds of all intrusions and accounts for nearly one-third of all [sensitive data] records compromised.'

Compensating Controls in PCI DSS

As we mention above, PCI mandates the implementation of hundreds of controls, often in a clearly prescriptive manner. What happens if an organization is unable to implement security in exactly the manner mandated by the DSS standard? The key concept here is "compensating control" which is defined in the standard as follows: *"Compensating controls may be considered for most PCI DSS requirements when an*

entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints." Here are some of the examples of PCI requirements that commonly use compensating controls (from the book "PCI Compliance" by the author of this whitepaper):

- Logging and log management (Requirement 10)
- Encryption of stored data (Requirement 3.4)
- Application security in case of internal applications (Requirement 6.5)

The key point to remember is that the compensating controls should be better or more secure than the original requirement and not simply be a poor substitute. Despite this strict definition, the QSAs in the field often have to deal with unsuitable and ineffective compensating control suggestions from the merchants.

Most Challenging PCI Controls – Ongoing Monitoring

According to Verizon PCI report, the logging and monitoring (Requirement 10), regular testing (Requirement 11) and encryption of stored data (Requirement 3) are the hardest to comply with and most often missing from organization worldwide.

What most of the above controls have in common are ongoing requirements! The controls that call for ongoing, daily effort are harder. Monitoring access to card data must be continuous to be effective against data breaches. The log review, the key part of Requirement 10.6, is explicitly mandated to be happening on a daily basis.

Technical controls are often evidenced by actual configuration files (technology proof), screen captures, logs and other IT data. Policy controls are evidenced by documented practices (and evidence of following them).

Let's consider a few real-world scenarios where the monitoring challenges discussed above come to an extreme.

Cloud Application Scenario

For cloud application that are accessed by IT users from their desktops, the monitoring at the cloud end might not be possible in many cases due to provider policies and practices. On top of this, getting logs and other monitoring data from a cloud provider might not have the granularity needed for PCI DSS. On the other side, if a browser is used to access the application (the most common route), the local logging will not be adequate either. As a result, a company will have an application that touches sensitive and regulated data which would not be able to monitor and won't have PCI-mandated logs to review.

Custom Application Scenario

Custom applications, scripts, including modified and open source payment applications, are still a reality at many merchants. In addition, stored credit card data, accumulated at branch offices and corporate data centers, is commonly accessed for various analytics purposes by other applications. These analytic applications, used by marketing departments, are often not written based on PCI-mandated security procedures. Many smaller merchant also chose to use the open-source and freeware application with regulated data. Monitoring these applications requires a different method, rather than rewriting the application to include logging.

Legacy Application Scenario

While mobile devices and Windows 7 desktops are a common sight across the IT landscape worldwide, many store environment as well as hotels, restaurants and even financial companies still use legacy platform and legacy applications for sensitive and regulated data processing. Over the years, these platforms, such as mainframes and mid-range systems, older servers and even Point-of-Sale (POS) terminals have been entrenched and are likely to be removed when they break down. Establishing PCI DSS compliance and implementing PCI controls, including security monitoring and log review, in such environment presents a unique challenge since many of these systems simply do not have PCI-prescribed security capabilities.

Monitoring legacy platforms and applications require actually *creating* all the audit information by the monitoring application that watches for user operations with regulated data.

Debugging Logs Only Scenario

Another common case is when an application in scope for PCI DSS does have logging, but such logging falls far short of compliance requirements. Inadequate logging is common in legacy application. Another common scenario is application where logging was designed purely for operational and debugging purposes and not for security and compliance audits. PCI DSS and other regulations imply that logs are clear records of user and system activity that can be used by internal security personnel and auditors to determine “who did what” with regulated data. Such logs must be granular, clear, and readable by the reviewers

In such cases, it is often easier to actually *create* all the audit information by the monitoring application that watches for user operations with regulated data and not trust the built-in inadequate logging.

Solving the Worst Case Monitoring Problems

The right solution for “cracking the nut” of PCI DSS controls and security for environments where logging and monitoring are next to impossible is in “making your own logs” where none exist or “making better logs” where logs are inadequate for facing the challenges. Technologies such as ObserveIT make that possible. ObserveIT auditing software acts like a security camera on your servers, creating logs and enabling PCI DSS monitoring. It does the following:

- make logs where none exist by recording text logs and video replay of every app (even apps with no internal logs!), over every session protocol (SSH, RDP, Citrix, VMware, etc.) on Windows, Unix and Linux
- enable better logging and achieve accountability when shared-user logins (ex: 'administrator') are tied to specific named users
- help you review and analyze the records by using compliance reports and build-your-own forensic searches that meet your compliance and security needs

Overall Observe IT has critical value for PCI compliance in the following domains:

- Provide external vendor access monitoring and gain insight exactly what 3rd party vendors are doing (PCI DSS requirement 8.5.6)
- Drastically simplify log review by creating “human readable logs” – and enhanced obscure system logs are by additional clear human-readable logs (Requirement 10.6)
- Tie each shared-user session recording to a specific named user (Requirement 10.1)
- Enable log creation where logs don't exist but monitoring is still mandatory: cloud application, legacy application and custom application with no own logging (Requirement 10)
- Simplify user policy monitoring (Requirement 12)

Finally, ObserveIT technology serves as a key compensating control for logging and monitoring in PCI DSS environment. Such solutions are indeed the only way to comply with Requirement 10 for the above scenarios. By being able to track every access to servers and databases, cloud applications, legacy and custom applications and, in essence, audit people and their actions and not just systems, Observe-IT follows the original spirit of PCI DSS. PCI DSS was created for protecting data from attacks and threat agents and your organization actions around PCI DSS should enable useful security monitoring and not simply record obscure system-level data.

Total PCI DSS control coverage by Observe-IT solutions can be found at the website.

Conclusions and action items

The key points to remember is that regulatory mandates compel organization to monitor their environment for security issues – even in the absence of simple way of doing so. In case of PCI DSS, monitoring of challenging environment can be accomplished by using applications that create logs, metadata and even screen capture videos of regulated data operations. On top of this, such technology can be used to "bulk up" logging for situations where existing logs are not adequate for incident investigations, security monitoring as well as fall short of regulatory requirements.

The actions items are:

- Review how you monitor cloud, legacy and custom application that touch regulated data
- Deploy technology to create or enrich existing audit logs for improved, compliant monitoring
- Review your PCI DSS compensating control for application monitoring, vendor activity and logging to make sure they satisfy PCI guidelines

About the author

Dr. Anton Chuvakin (http://www.chuvakin.org) is a recognized security expert in the field of log management and PCI DSS compliance. Anton leads his security consulting practice www.securitywarriorconsulting.com, focusing on logging, SIEM, security strategy and PCI DSS compliance for security vendors and Fortune 500 organizations. He is an author of books "Security Warrior" and "PCI Compliance" and a contributor to "Know Your Enemy II", "Information Security Management Handbook"; he is now working on a book about computer logs. Anton has published dozens of papers on log management, correlation, data analysis, PCI DSS, security management (see list www.info-secure.org) . His blog http://www.securitywarrior.org is one of the most popular in the industry.