Ovum
TMT intelligence | informa

Making Sense of Compliance: Securing Card Payments with the PCI DSS

Best practices for compliance and corporate governance

Publication Date: June 18, 2018

Rik Turner

Ovum view

Summary

The Payment Card Industry Data Security Standard (PCI DSS) is the most important information security standard for companies that handle credit and debit cards. It is set by the PCI Security Standards Council (PCI SSC), which comprises Visa, Mastercard, American Express, Discover, and JCB, and can therefore claim to be a global standard. This white paper looks at what it takes for merchants and data processors to comply with version 3.2 that was published on April 28, 2016. Minor revisions were made to this version and published on May 17, 2018 and although version 3.2.1 replaces v3.2, no new requirements were added.

The essence of the PCI's security standard is the protection of customer data that, if compromised, could be used for fraudulent activity on a payment card account. For merchants and service providers, compliance with the standard requires annual validation via audit. Therefore, technology that can selectively omit all sensitive data (see below for definition) from the call recordings used in contact centers for purposes of customer service effectively reduces the scope of that audit. Ovum encourages all companies that need to demonstrate compliance with the PCI DSS to consider deploying such a capability.

What is the PCI DSS?

The history

The origins of the PCI DSS date back to 1999, when Visa USA established the Cardholder Information Security Program (CISP) to ensure the security of cardholder information as it was being processed and stored by merchants and service providers such as payment processors. The other four major card brands followed suit, introducing their own security programs.

All this activity was in response to a growing number of breaches in which credit card details were stolen due to poor practices, such as the use of default passwords and weak network security, or storing cardholder data in the same place as all other corporate information assets.

With each credit card brand developing its own rules for securing data, however, merchants soon began to call for commonality to make it easier (and cheaper) to comply, to which end the PCI DSS was created as a proprietary standard (i.e. not ratified by an international standards body), with each brand bringing its policies in line with the overall standard.

The first version of the standard (v1.0) was released on December 15, 2004. The PCI SSC, also known as the PCI Council, was formed in 2006 to oversee the development of the standard.

The emergence of PA-DSS

A further standard under the Council's control is the Payment Application Data Security Standard (PA-DSS), which came into existence in October 2009, incorporating work previously done in a proprietary fashion by Visa called the Payment Application Best Practices (PABP).

This standard came about in response to the development of electronic payment platforms for card-present and, in particular, card-not-present transactions. It addresses software vendors that develop payment applications and is designed to prevent such applications from storing secure data such as

magnetic stripe, CVV2, or PIN. It also dictates that software vendors develop payment applications that are compliant with the PCI DSS.

Compliance and compliance testing

Although the PCI DSS must be implemented by all entities that process, store, or transmit cardholder data, formal validation of PCI DSS compliance (PCI compliance for short) is not mandatory for all entities. However, both Visa and Mastercard currently require merchants and service providers to be validated according to the PCI DSS.

Compliance with the standard is tested by a Qualified Security Assessor (QSA), a person certified for the role by the PCI Council. The QSA performs an audit and prepares a Report on Compliance (ROC), with only merchants that have been judged compliant by the Assessor being able to receive credit card payments. Furthermore, merchants and service providers are required annually to fill in a Self-Assessment Questionnaire (SAQ) attesting to their ongoing compliance.

Issuing banks are not required to go through PCI DSS validation, but they must still secure sensitive data in a PCI DSS-compliant manner. Acquiring banks, on the other hand, are required to comply with the PCI DSS, as well as to have their compliance validated by audit.

What are the PCI DSS's key features?

The 12 top-level requirements

Since its inception, the standard has maintained 12 overriding requirements for protecting cardholder data. These are listed in Table 1.

Table 1: PCI DSS requirements

Goals	PCI DSS requirements
Build and maintain a secure network and systems	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
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 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 processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

Source: Verint

The standard must keep up with new technologies and new threats

As technology continues to evolve, so too do the security challenges implicit in handling payment cards. For this reason, over time the PCI DSS has been extended, gaining new attributes and, in some cases, even entirely new dimensions. The Council draws on input from 700 so-called Participating Organizations (comprising merchants, banks, processors, hardware and software developers, and point-of-sale vendors) to determine how the standard needs to evolve.

Thus, in July 2009 the Council introduced security guidelines for the scenario in which cardholder data traverses a Wi-Fi network, which include recommending the use of a wireless intrusion prevention system (WIPS). Similarly, in March 2011 it issued an FAQ on call recording in contact centers, specifying that companies must not store digital recordings that include sensitive card data if those recordings can be queried.

Version 3.2 introduces an MFA requirement

Version 3.2 of the PCI DSS introduced a series of enhancements, the most significant of which is multi-factor authentication (MFA) as a requirement for any personnel with administrative access into environments handling card data. Previously, the requirement was for two-factor authentication (2FA), and applied only to remote access from untrusted networks.

Other clauses in v3.2 include a requirement to encrypt all non-console administrative access using strong cryptography, and another to use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

How can technology help with PCI DSS compliance?

As the PCI Council itself says, compliance with the DSS requires a combination of people, processes, and policy, with technology supporting all three elements.

The sponsor of this white paper, Verint Systems, develops technology for the capture and analysis of communications. In the context of the PCI DSS, it has products to enable compliance in the contact center, where sensitive cardholder data such as the card validation code/card security code is routinely exchanged between callers and agents.

The relevant Verint products for PCI compliance are as follows:

- **Verint Call Recording:** This is where conversations can be recorded and stored in a secure, encrypted form.
- **Verint Interaction Data Export/Import Manager:** An application for importing calls from third-party recorders into the Verint recording system.
- **Verint Encryption Management:** The application that communicates with the Verint recorder and/or the Import Manager to encrypt files being recorded, caching the encryption keys in the recorder, while the encrypted files can, as dictated by the customer's retention policy, be archived to a centralized, permanent storage facility managed by the Verint Central Archive Manager (CAM).
- **Verint Speech Analytics:** This is where transcribed audio files are ingested for analysis.
- **Verint Screen Capture:** This is an application for recording information from a contact center agent's computer screen.

- **Verint Advanced Desktop Analytics:** This is Verint's application for providing companies with visibility into how employees use software applications. While it can be used to identify top performers and measure volumes, activity, and process flows in a contact center, it is also a valuable tool for identifying irregular behavior around sensitive data.

The capture and secure storage of voice data is, of course, what Verint is best known for in the market, along with the ability to analyze all this recorded information for business and/or governance insights. However, in the case of PCI compliance, there is considerable emphasis on what information must **not** be recorded and stored, so it is just as important from this perspective that Verint platforms know when not to proceed with recording.

In this context, therefore, Verint Call Recording provides an integration interface to allow users to instruct recorders to briefly stop (or pause) recording the audio and screen while sensitive information, such as the card validation code/card security code, is being relayed verbally. The software automatically detects when sensitive and private information is about to be exchanged between the customer and the contact center agent/employee and can proceed, either not to capture it or, if it can be captured, to securely store and archive it.

One of the advantages of the "pause and resume" approach to sensitive data in the contact center scenario is that it reduces the scope of the PCI compliance audits performed by QSAs. In other words, if a company has already shown in a previous audit that it is not recording sensitive data thanks to this mechanism, it will not need to be audited again.

Appendix

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo