

White Paper

Managers' Cheat Sheet for PCI DSS

Introduction

PCI DSS stands for Payment Card Industry Data Security Standard. This standard was developed at the urging of large credit card companies to help organizations that process credit card payments to prevent privacy and security breaches through hacking and other means.

The standard became mandatory for all companies that process credit card payments in 2008. Compliant companies have protected their networks and web applications and all such companies must verify their compliance at least once per year, and more often for companies processing higher volumes of transactions.

There is a common perception that PCI compliance involves following a complex and onerous set of regulations, but this perception can be misleading. While PCI compliance can be challenging to achieve, for those companies already undertaking best practices for corporate security and privacy, compliance can be a matter of adjusting procedures and processes in very minor ways.

Rather than a comprehensive report, this white paper aims to provide guidance on key questions about the PCI DSS regulations.

Questions about PCI DSS

These are some answers to common questions about PCI DSS.

What is PCI DSS?

Payment Card Industry Data Security Standard. Sometimes, shortened to PCI or PCI compliance.

PCI DSS is a set of comprehensive requirements for enhancing payment account data security, developed by the PCI Security Standards Council, which includes American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International. Since then, there have been a number of changes to the regulations. For instance, PCI DSS regulation 6.6 made PCI compliance for web applications mandatory as of June 30, 2008.

PCI DSS helps facilitate the broad adoption of consistent data security measures around the world. The standard helps assure customers using credit cards that the steps are in place to protect their information and privacy, which is under threat from hackers and cyber criminals.

What are the requirements of PCI DSS?

The focus of PCI DSS is on protecting the network and web application access so that credit card data is not compromised. There are many specific requirements, but that should not mislead vendors into hesitating to adopt PCI DSS standards.

Companies that already follow industry-standard best practices for privacy and security will not have to undertake onerous changes to their operations. At the same time, companies that have not taken these issues seriously until now face mandatory regulations to harden their systems and procedures against a breach as quickly and comprehensively as possible.

The basic requirements of PCI DSS are listed below:

- **Build and Maintain a Secure Network**

Organizations must install and maintain a firewall configuration to protect cardholder data. As well, they should not use vendor-supplied defaults for system passwords and other security parameters.

- **Protect Cardholder Data**

Organizations are required to protect stored cardholder data and encrypt transmission of that data across open and public networks.

- **Have a Vulnerability Management Program**

You must use and regularly update anti-virus software. Again, this is not only good practice for PCI compliance, but generally for protecting your business. As well, PCI rules mandate that organizations develop and maintain secure systems and applications that protect against known vulnerabilities that hackers can exploit.

- **Deploy Robust Access Controls**

Access to cardholder data by business must only be restricted to those with a need-to-know basis. Every member of your organization with computer access should be given a unique ID. As well, steps must be taken to restrict physical access to cardholder data. For instance, physical locks and security personnel may be required to secure access to rooms with databases or servers containing credit card information.

- **Monitor and Test Networks**

PCI-compliant organizations must track and monitor access to network assets and cardholder data. This will not only improve security, but also help identify the cause of a breach should it occur. Security systems and processes must be regularly tested to ensure their ongoing effectiveness.

- **Maintain an Information Security Policy**

It is not enough to have technology tools like a firewall or network audit applications to protect private information. Improper handling of information by untrained staff is a huge security vulnerability. Security policies must be developed, implemented and regularly updated.

Why was PCI DSS developed?

Privacy and security breaches involving credit card transactions pose a clear danger to credit card companies and financial institutions. If the general public begins to feel that credit card payments are fundamentally insecure, they will stop using them.

These institutions then put pressure on the vendors that process these payments. Companies that are not PCI compliant can be subject to heavy fines enforced by the credit card companies.

How exactly do the credit card companies pressure businesses to protect consumers' data?

Merchants found to be non-compliant with PCI DSS may be levied fines by credit card companies. Acquiring banks may also contractually oblige merchants to indemnify and reimburse them fines paid from bank funds on behalf of the non-compliant merchant. Fines may

be as high as \$500,000 per privacy and security breach if merchants are discovered to be non-compliant.

For example, in 2006, Visa alone levied almost \$5 million in fines. In 2007, Visa levied a \$880,000 penalty against the bank involved with TJX's privacy and security breach ("Are You Compliant?", Small Business Online Community).

In the worst case scenario, merchants could also risk losing the ability to process customers' credit card transactions.

What are the PCI DSS merchant levels?

Merchants fall into four categories. The first level is for merchants processing over 6 million transactions per year. It can also apply to a company that the credit card company believes should have to meet Level 1 merchant requirements to reduce risk for the credit card company.

Level 1 merchants require an annual on-site PCI DSS assessment and quarterly network scan by a Qualified Security Assessor (QSA) or Internal Audit, plus an Approved Scanning Vendor (ASV) (Visa, "Cardholder Information Security Program).

The second level is for merchants processing one million to 6 million transactions. Level 3 is for merchants processing 20,000 to one million transactions. Level 4, which applies mainly to small businesses, is for merchants processing fewer than 20,000 credit card e-commerce transactions per year. All merchants from any level must have some kind of PCI assessment and quarterly network scan. At the highest level, Level 1, the validation must be done by a QSA and ASV, while lower-level merchants can be validate through a combination of self-assessment and use of an ASV.

It is important to note that any merchant that has suffered a breach that resulted in an account data compromise may be escalated to a higher validation level.

How many organizations are actually PCI DSS compliant?

Exact figures are not known, but based on a number of recent studies such as "The State of PCI Compliance" by Forrester Research, it is clear that many companies still haven't begun to prepare for PCI compliance. According to the Forrester study, less than a quarter of surveyed companies in the US, UK and Europe in late 2007 had passed a PCI audit and most had only completed one or two stages leading up to PCI compliance, such as a security gap analysis. It is unclear whether the change in regulations to make PCI compliance mandatory will change the landscape.

Conclusion

PCI DSS mandatory regulations affect a large swathe of companies across a number of industries. However, a lack of clear understanding amongst companies about PCI regulations may have contributed to a delayed adoption of compliance standards.

Better understanding of PCI DSS will expedite adoption of these best practices. Companies are encouraged to seek further assistance about PCI from public sources such as the PCI Security Standards Council (<https://www.pcisecuritystandards.org/>) and from credit card companies which have published information about the regulations merchants must follow.

PCI compliance may seem complicated at first, but for companies that already have good tools, policies and procedures for protecting private information on their network, these regulations may not be a difficult standard to reach. By following industry-standard best practices for IT security, PCI compliance becomes a non-intrusive checklist to ensure companies are on the right path to protecting themselves and their customers.

Works Cited

Forrester Research. "The State of PCI Compliance".

http://www.rsa.com/solutions/PCI/ar/RSA_AR_State_of_PCI_Compliance.pdf

Richardson, Reed. "Are You Compliant?" Small Business Online Community. April 17, 2008.

<http://smallbusinessonlinecommunity.bankofamerica.com/blogs/merchantServices/2008/04/17/are-you-compliant>

Visa. "Cardholder Information Security Program".

http://usa.visa.com/merchants/risk_management/cisp_merchants.html

Wikipedia. "PCI DSS". http://en.wikipedia.org/wiki/PCI_DSS

About

Pacific Coast Information Systems Ltd.

Pacific Coast Information Systems (PCIS) Ltd. is a full-service technology and consulting firm based in Vancouver. Founded in 1995, PCIS provides technical assessment & services, business analysis, and IT project management. More information about PCIS can be found at www.pcis.com

Boonbox

Boonbox, a division of PCIS, was created in 2007. Boonbox specializes in productivity solutions that deliver immediate results in support of business challenges like security compliance, password protection and data backup issues. More information about Boonbox can be found at www.boonbox.net