Sense and Security in PCI DSS Compliance: Cases from the Asia-Pacific Region

Wen Li CHAN[1]*, Cristina YAP[2] and Hsin-Vonn SEOW[1]

[1]Nottingham University Business School, University of Nottingham Malaysia Campus
[2]Vectra Information Security

**Correspondence: Wen Li Chan, Nottingham University Business School, University of Nottingham Malaysia Campus, Jalan Broga, 43500 Semenyih, Selangor, Malaysia. E-mail: wenli.chan@nottingham.edu.my*

Keywords: Data security, Data security standard, Payment cards, Payment card industry, PCI DSS.

Extended Abstract

The payment card industry plays an important role in global commerce, with the use of non-cash payments steadily on the rise. Global non-cash transaction volumes increased by 11.2% during 2014–2015 to a figure of 433.1 billion, reported to be the highest growth of the past decade (Capgemini and BNP Paribas, 2017). In Southeast Asia, Singapore leads the region in terms of consumers' preference for using payment cards over cash, with 76% of consumers in a Visa survey preferring to use payment cards over cash (Visa, 2015).

In the consumer market, payment card systems involve interrelationships between consumers (cardholders) who use payment cards, and merchants who accept payment cards as a mode of payment. A persistent issue in the payments industry is that of data security breaches, which impact both the consumer and merchant sides of the consumer payments landscape. The compromised data of consumers is vulnerable to use in fraudulent spending and fraudulent financial applications taken out in the names of stolen identities. In the case of merchants, the losses associated with each stolen record involves losses in revenue due to fraudulent charges, and also intangible losses such as brand damage, the loss of existing customers and the decline in new customer acquisitions (Smart Card Alliance Payments Council, 2015).

The PCI DSS (Payment Card Industry Data Security Standard) was created in the wake of high-profile data security breaches in the early 2000s, in a bid to promote and improve on the safeguards available to prevent such security breaches to systems that store cardholder data and account information. The PCI DSS is a unified security standard enforced by the five major payment card associations – American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. – in respect of payment cards issued by these five organisations. PCI DSS compliance assessments are carried out by qualified assessors to evaluate whether a business has the relevant security standards and practices in relation to the storing, processing, and transmission of data in transactions made via a payment card.

To be compliant with PCI DSS, merchants and service providers are to meet twelve requirements around building and maintaining secure networks and systems, cardholder data protection, vulnerability measurement measures, access control management, monitoring and testing, and information security policies, which are further detailed into sub-requirements. The implementation of PCI DSS has not been smooth-sailing, with many companies citing cost as a hurdle (Morse and Raval, 2008; Everett, 2009), in

particular the cost required to undertake necessary remediations to attain compliance (Rees, 2012) although, arguably, the costs may outweigh the potential tangible and intangible losses that could result in the event of a security breach.

The PCI DSS on-site assessment process is carried out by qualified assessors based on a given scope. To be efficient, audit programmes should aim to reduce the effort required for assessing the compliance position of the organisation, whereby for areas where sufficient documentation is available, audit activities may be reduced to spot checks that validates the coherence and accuracy of supplied documentation (Ataya, 2010).

With this in mind, we examine the issues faced in the case of several merchants and service providers based in Singapore over two cycles of PCI DSS compliance assessments, by regressing twenty common pitfalls recorded during the initial stages of each of the audit cycles where gaps are identified, and the time taken to achieve compliance as independent variables against the dependent variable of whether the companies achieved compliance, to determine the weightage of each independent variable in contributing towards achieving PCI DSS compliance. We compare the results with the issues faced by these organisations across the two audit cycles and through changes dictated by shifting threat vectors to shed light on ways in which PCI DSS assessments can be facilitated for certain types of businesses, that would make for more effective utilisation of the resources involved in such assessments and pave the way for improving the data security landscape. We conclude with some recommendations on best practices moving forward to better achieve the objectives which the PCI standards set out to meet.

References

Ataya, G. (2010), 'Review – PCI DSS audit and compliance', *Information Security Technical Report*, Vol. 15, pp.138-144.

Capgemini and BNP Paribas (2017), *World Payments Report 2017 – A preview into the global payments landscape*, accessed on 16 July 2017 at www.worldpaymentsreport.com

Everett, C. (2009), 'PCI DSS: Lack of direction or lack of commitment?', *Computer Fraud & Security*, December 2009, pp. 18-20.

Morse, E. A. and Raval, V. (2008), 'PCI DSS: Payment card industry data security standards in context', *Computer Law and Security Report*, Vol. 24, 540.554, pp. 540-554.

Rees, J. (2012), 'Tackling the PCI DSS challenges', *Computer Fraud & Security*, January 2012, pp. 15-17.

Smart Card Alliance Payments Council (2015), *The True Cost of Data Breaches in the Payments Industry*, A Smart Card Alliance Payments Council White Paper, No. PC-15001, March 2015, accessed on 15 July 2017 at https://www.securetechalliance.org/wp-content/uploads/The-Cost-of-Data-Breaches.pdf

Visa (2015), *The Road Ahead – Consumer Payment Trends in Southeast Asia*, accessed 15 July 2017 at http://www.visa.co.id/aboutvisa/research/include/The_Road_Ahead_Report_IPV_ID.pdf