International Journal of Information & Network Security (IJINS)
Vol.2, No.2, April 2013, pp. 118~123
ISSN: 2089-3299

PCI Compliance – No excuses, please

Martin Harran*, Nigel McKelvey*,
* Department of Computing, Letterkenny Institute of Technology, Port Road, Letterkenny, Co Donegal, Ireland.

Article Info

Article history:

Received Nov 10th, 2012
Accepted Dec 10th, 2012

Keyword:

PCI Compliance
Security
Fraud
Credit Cards
Cost of Compliance

ABSTRACT

PCI Compliance is an area of particular concern for companies considering moving some of their activities onto the Cloud. This paper discusses how such concerns are really nothing new, that they are simply the latest manifestation of underlying friction that has long existed between merchants and payment card processors. The paper reviews the most common complaints made by merchants and shows how they are largely based on misunderstandings of the purpose and nature of the compliance procedure and argues that any company with a sound approach to security should have little problems with the process. It concludes that properly understood and applied, the PCI Compliance process can be of real benefit to businesses not just in absolute terms of achieving compliance but as a good starting point in developing a more effective overall approach to security.

Corresponding Author:

Nigel McKelvey,
Department of Computing,
Letterkenny Institute of Technology,
Port Road, Letterkenny, Co Donegal, Ireland.
Email: nigel.mckelvey@lyit.ie

1. INTRODUCTION

PCI Compliance has become something of an issue recently with companies looking at cloud computing and unclear about the potential impact on their PCI Compliance. It is difficult to see why companies have any doubts where responsibilities lie when compliance responsibility clearly rests absolutely on the merchant [5]. This uncertainty appears to be just the latest example of PCI Compliance being viewed or represented as something other than what it is - a problem that long predates the cloud. This article reviews some of the more common complaints that merchants make and the sometimes fundamental lack of security awareness that underlies them.

2. COMPLAINT 1: PCI COMPLIANCE DOES NOTHING FOR SECURITY

This is often based on the observation that at least one well known company was hacked the very day they got their compliance and involves several layers of misunderstanding.

Firstly, PCI Compliance has nothing to do with making a company more secure, it is a procedure with one purpose - to protect the card issuing companies. Compliance can be compared to somebody getting their house robbed – the occupants might undergo all sorts of horrors and have valuable possessions stolen but if the robbers don't get hold of their credit cards, compliance has been achieved and the card company have no interest in the matter. That is not to say that the procedure has no benefits for the merchants; on the contrary, it can provide a good starting point for smaller businesses in developing a security awareness culture but the starting point has to be that PCI Compliance procedures are designed for the benefit of the card issuers, meeting the requirements is part and parcel of using their services.

The second misunderstanding is that compliance is designed to prevent security breaches. It isn't – it is only designed to assess how well a company is managing security. Like an insurance company checking if premises have a burglar alarm, it is about risk reduction - the best alarm systems in the world will not defeat a determined criminal but businesses or homes with weak security systems are the ones most likely to get

robbed. Credit card fraud is similar; card issuing companies know that it is impossible to make any business totally secure but those with the weakest systems are those most likely to get attacked. This is shown in the statistics for credit card compromises – figures for 2009 showed that 80% of all data compromises identified since 2005 had happened with Level 4 merchants, i.e. the smallest companies, and that less that 5% of potentially exposed accounts had actually been compromised [1].

The third misunderstanding is that compliance is a perpetual state. Compliance only refers to the point in time where the systems were assessed. It is like a medical examination – a clean bill of health only refers to the time that the doctor did the examination; it only applies within the limits of the tests actually carried out by the doctor and it gives no guarantee about their future health. Regular medical test do not mean one cannot become seriously ill but they can highlight specific risks at an early stage; PCI Compliance does the same in regard to the health of a company's payment handling systems.

It is worth noting that despite much public criticism following the highly publicised 2008 compromise in Heartland – the fifth largest credit card processor in the USA, handling over 11 million transactions per day - Ellen Richey, chief enterprise risk officer for VISA, insisted that "no compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach." [8]

3. COMPLAINT 2: PCI COMPLIANCE IS AN UNNECESSARILY ONEROUS PROCESS

It is difficult to see how merchants can justify this claim. The 12 requirements for compliance are shown in Figure 1 – these are basic elements of any data security system and should be in place irrespective of any need for compliance. Michaels Stores has over 1000 outlets in North America with net income of $176M in 2001 on turnover of just over $4 billion so it would seem reasonable to expect them to have top notch systems where PCI compliance would be the proverbial dawdle. Their CIO, Michael Jones, however, complained strongly about the demands of the procedure to a Committee on Homeland Security hearing in March 2009 assessing the impact of PCI Compliance, stating that "(...the PCI DSS requirements...) are very expensive to implement, confusing to comply with, and ultimately subjective, both in their interpretation and in their enforcement. It is often stated that there are only twelve 'Requirements' for PCI compliance. In fact there are over 220 sub-requirements; some of which can place an incredible burden on a retailer and many of which are subject to interpretation." [2].

Jones talked at length about his company's need to store credit card numbers as a means of handling chargebacks. He did not, however, specify which particular steps in the procedure could be regarded as unnecessary in any security system for handling payments or which ones involved excessive cost in relation to a company the size of Michaels Stores and finished up by stating : "In conclusion, I am proud to report that Michaels has never had evidence of a breach of consumer data. Regardless of the outcome here, we will continue to do what is necessary. "

Unfortunately for him and his company, just two years later they admitted to a major security breach with systems comprised in 20 states over a 3 month period the effects of which rumble on with the continuing class action instigated against the company on behalf of affected customers. Also, in what was perhaps a tribute to the onerous procedures complained about, less than 100 cards ended up being reported as actually used in fraudulent transactions. [4].

Figure 2 shows the actual levels of compliance for the various Merchant Levels in the USA as reported by VISA in June 2012. The results for Level 1 Merchants show that for the vast majority – 97% - the procedures certainly did not seem to be overly onerous, at least not enough to stop them achieving compliance. These, are the largest 400 companies in the USA it terms of card transactions and, with turnover of many $ millions, one would expect highly robust procedures to be in place as a matter of course; indeed, one has to wonder what possible excuses could be accepted from the dozen or so companies at this level who failed to achieve compliance.

Performance was less satisfactory with Level 2 clients but was still 93%. Although these companies are smaller and undergo a less severe scrutiny – their compliance is based on self assessment rather than requiring the involvement of an external Qualified Security Assessor (QSA) - their turnover is still in multiple $ millions and many of them probably aspire to achieve Level 1 turnover. Such companies have to understand that having sound security systems a vital component in achieving that kind of growth and it has to be recognised that less than 10% of companies fail to do so. Like Level 1, there seems little excuse for companies of such size failing to reach the required standards.

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	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. Use and regularly update anti-virus software on all systems commonly affected by malware
	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. 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 processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Figure 1. Compliance Requirements
Based on PCI Compliance Guide, n.d.

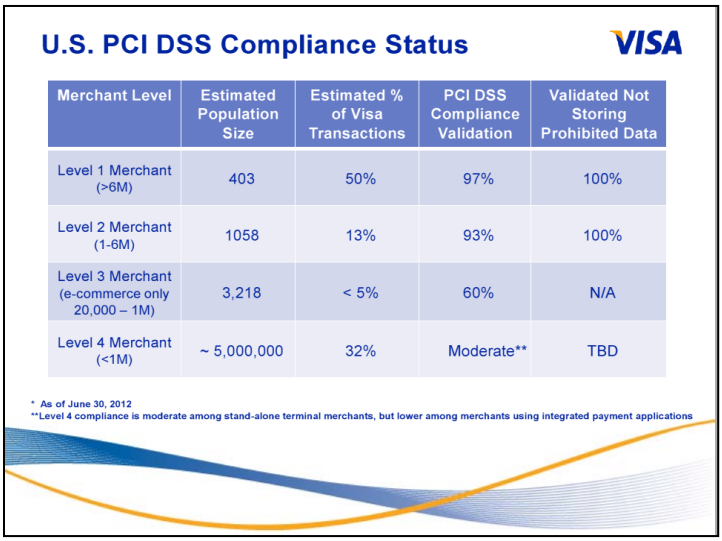

Figure 2: Compliance Levels [9]

Level 3 Merchants are entirely e-commerce with between 20K and 1M transactions per year and only 60% of such merchants achieved compliance for the period. No explanation is given for such a low result but at less than 5% of all transactions, this group is effectively a subset of Level 4 and many of the same factors will apply. Level 4 Merchants process an average of less than 1 million transactions per year, the majority of them considerably less than that – a 2009 survey of merchants carried out by ControlScan, the National Retail Federation (NRF) and the PCI Knowledge Base showed that almost half of them process less than 100,000 card transactions per year and 57% only have 1 to 10 employees [3].

VISA don't give an actual figure for compliance among this group, simply describing it as "moderate" but there is no reason to think that it is any better than Level 3. Many if not most of these merchants are in the 'mom and pop shop' category, unlikely to have much IT knowledge and not large enough to support professional IT assistance. This, however, seems little excuse for achieving required standards of security. Somebody setting up a pizza parlour may know very little about hygiene legislation but they are going to have to find out very quickly and make sure they comply with the requirements; is it any less reasonable that if they are going to carry out payment card transactions which may seriously affect the financial "health" of their suppliers and customers, that they should put equal attention into finding out and complying with the equivalent requirements?

The merchants do recognise the importance of compliance; 78% of respondents of the to the survey by ControlScan et al. agreed that the PCI standards should apply to their business but lack of real understanding of the process is a significant problem with only 44% stating that they were "very familiar" with it. This is clearly an area where the card companies need to do more work. A secondary statistic provided by the survey indicates that the banks have a captive audience here – 77% of merchants turn to their bank and 66% turn to their Point of Sale/Payment Application Vendor for advice on compliance.

4. COMPLAINT 3: IT COSTS TOO MUCH

PCI Compliance does not come cheap with an estimated annual cost of $2.7 million for an average Level 1 company [7]. This cost, however, has to be looked at relative to overall revenue. A mid-range Level 1 merchant handles around 3 million transactions per year. At even $10 per transaction, that means revenue in excess of $30 Million which takes compliance cost to less than 10% of revenue; actual transaction values are likely to be multiples of that which means that the compliance cost is probably only a very small percentage of costs. Costs for other levels is substantially less in absolute terms – the Level 4 survey showed that 41% of respondents had spent less than $500 to achieve compliance and another 29% less than $5000. An interesting statistic from the same report was that among respondents who had experienced a data breach, 69% spent $501-$5000 for compliance whereas that level of cost was only incurred by 26% of those who had not experienced a breach. As pointed out in the survey:

"Small businesses with few resources may be prone to cut corners on costs, especially when they don't understand the risks and the consequences. This is the security equivalent of buying fire insurance after a fire."

The potential cost of a breach is something that companies cannot ignore. Average costs of a security breach in the USA in 2010 were estimated at $6.75 million with the most expensive incident costing $31 million [6]. These costs are for all types of breaches, not just payment cards but they do give an indication of the potential costs involved. There is another potential cost to be added in – litigation and damages. Michaels Stores are still in the process of fighting the class action taken against them in regard to their 2011 data breach. Whatever the costs, companies cannot wish them away any more than rent or wages or any other overhead, just like other costs they have to be factored into the overall cost of doing business.

5. COMPLAINT 4: THE CARD COMPANIES CONTRADICT THEMSELVES

This complaint contains two elements of truth but juxtaposes them in a way that presents a less than accurate picture. Taking the second point first, the card issuers do not ask for data storage in any electronic form, they simply insist that if a merchant wants to be able to refute a proposed chargeback (refund) where a customer has challenged a payment, then the merchant must be able to produce a copy of the paper receipt for the transaction. Whilst these paper receipts must be stored in a secure way, they actually contain very little security sensitive data, usually only showing the last 4 digits of the payment card number; storing them securely is essentially no different from storing any other financial records in a business. Where the problems arise is when companies decide to additionally store data in an electronic form. The Michaels Stores CIO at the Homeland Security hearing, for example, appeared to suggest that the company was storing the actual credit card numbers to make it easier for them to track down a particular receipt. He also sated that these

receipts are the company's best means of minimising chargebacks – "Often, once the customer sees the underlying documents he remembers the purchase and the matter is closed."

The PCI Compliance requirements state that the merchant should seek to avoid storing credit card numbers but if it chooses to do so then the data must be encrypted. There is nothing new in that, encryption of sensitive data is a fundamental step in any security process.

6. COMPLAINT 5: THE COMPLIANCE PROCEDUE DOESN'T TAKE CLOUD INTO ACCOUNT

Again, this shows a fundamental misunderstanding of PCI Compliance – it is about how good a company is at security, not the specific technology which it chooses to implement. Essentially, if a company decides that it needs to store credit card data, the compliance procedure doesn't care whether the data is stored on a server in the company's back office or a virtual server 5000 miles away in Florida. All the procedure cares about is who has access to that data and whether it is encrypted.

The questions raised about PCI Compliance and the cloud also reflect a general lack of understanding about the cloud. For example, companies assume because their cloud provider is compliant, that should be enough. A cloud provider being compliant simply means that they are compliant in their own charging procedures, there is no 'trickle down' to their customers nor can there be for transactions in which the cloud provider has no direct involvement.

Some of the questions asked also reveal short sightedness about the wider impact on a company's operations. For example, if a UK based company decides to move its operating systems onto a virtual server in the USA, it has to think about much more than just the impact on PCI Compliance – does the location of the server create a legal entity in the USA with possible taxation implications? ... Which jurisdiction will apply for consumer law? … What if an employee is found committing an illegal act on the server, will the company be subject to UK or USA legislation? ... these are just some of the myriad of questions that should be considered before any move to cloud computing.

7. THE CARD ISSUERS DON'T TAKE THEIR FAIR SHARE OF THE BURDEN

This is perhaps the most well-grounded complaint - security for handling payment card transactions lies squarely with the merchants but that does not excuse the card issuers for not doing everything they can to improve things.

At one end of the scale, the Michaels Stores CIO has pointed out a relatively straightforward change to the issuers' procedures – the implementation of a unique transaction id – that would completely obviate the need for merchants to store any credit card data. At the other end of the scale, there is the lethargy that has been shown by them in introducing Chip and Pin cards. The Chairwoman of the Homeland Security hearing pointed out that over the 3 years following their introduction in the UK, credit card fraud was reduced by 67 percent, from 219 million pounds in 2004 to 73 million pounds in 2007. Despite these dramatic results, also seen in other countries, the USA has still not implemented Chip and Pin on any significant scale.

8. CONCLUSION

In looking at the reaction to PCI Compliance, it is possible to see similarities with other aspects of commercial history. For example, when employment legislation was radically overhauled in the 1970s with the introduction of major swathes of new employee protections, there was near uproar throughout the business world with claims that this was going to incur massive costs for larger companies and drive smaller ones out of business. This didn't happen and, as companies got used to the new legislative environment, they discovered that far from the legislation proving excessively onerous, embracing it in a positive manner and going beyond the bare compliance demands actually led to far better Human Relationships and improved business performance. The same principle applies to PCI Compliance. The standards are based on good and sensible security practices.

The world has changed; a generation ago, many small businesses did not have a need for alarm systems and roller, today they do. The less tangible business world has changed too and the simple levels of trust that once existed between retailer, customer and the bank no longer exist, we now operate in a e-jungle with many predators, one that will only get worse in the years ahead.

Achieving and maintaining the PCI standards is not an easy task but approaching it with a positive mind rather than seeking to get away with the bare minimum is a good step towards enabling a company to succeed in that jungle.

REFERENCES

[1] Bank of America, 2009. [online] Protecting Your Customer's Card Data. Available at: http://controller.ucsf.edu/cash_handling/files/Payment_Card_Industry_Data_Security_Standards.ppt [Accessed 09 October, 2012]

[2] Committee on Homeland Security, 2009. [pdf] Do the Payment Card Industry Data Standards Reduce Cybercrime? – Hearing Available at: http://www.homelandsecurity.house.gov/hearings/index.asp?id=185 [Accessed 08 November, 2012]

[3] ControlScan, the National Retail Federation (NRF),PCI Knowledge Base, 2009. [pdf] What Small Merchants Know (and Don't Know) about PCI Compliance. Available at http://www.nrf.com/modules.php?name=Documents&op=viewlive&sp_id=3539 [Accessed 09 October, 2012]

[4] Mail Tribune, 2011. [online] Michaels investigates customer data breach, replaces debit pads Available at: http://www.mailtribune.com/apps/pbcs.dll/article?AID=/20110514/BIZ/105140302 [Accessed 09 October, 2012]

[5] PCI Compliance Guide, n.d. [online] Q: Do organizations using third-party processors have to be PCI compliant? and THE BASICS OF PCI COMPLIANCE AND VALIDATION REGULATIONS Available at: http://www.pcicomplianceguide.org [Accessed 08 November, 2012]

[6] Ponemon, 2010. [pdf] Five Countries: Cost of Data Breach. Available at http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf [Accessed 09 October, 2012]

[7] TrustNet, ca. 2011. [online] Cost of PCI Compliance. Available at: http://www.trustnetinc.com/Compliance/cost-of-pci-compliance.html [Accessed 09 October, 2012]

[8] Jaikumar, V. 2009. [online] Visa: Post-breach criticism of PCI standard misplaced Available at: http://www.cso.com.au/article/296278/visa_post-breach_criticism_pci_standard_misplaced [Accessed 09 October, 2012]

[9] VISA, 2012 [pdf] U.S. PCI DSS Compliance Available at: http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf [Accessed 09 October, 2012]

BIOGRAPHY OF AUTHORS

First author's Photo (3x4cm)	Martin Harran – final year student studying a BSc in Applied Computing at the Letterkenny Institute of Technology, Ireland.
Second author's photo(3x4cm)	Nigel McKelvey – Computing Lecturer at the Letterkenny Institute of Technology, Ireland.