Article for Talking Payments

April 2015
Version 1.0

"PCI DSS. Bypassing the myths and going straight to what you really need to know"

By John Greenwood of Compliance3, a specialist PCI-DSS compliance service provider to contact centres.

The Payment Card Industry Data Security Standard (PCI DSS) aims to secure cardholder data that is stored, processed or transmitted by merchants and card processers. From the 1st July 2015, PCI DSS 3.0 will be the sole iteration of the standard that applies requiring businesses to document its Card Data Environment (CDE). That means mapping all areas that touch card data, and include contact centres if payments are taken over the phone.

However being PCI DSS compliant is NOT a tick box exercise. Nor is it a purely technology fix. "Security isn't about checking a box to pass an annual audit. It's about ongoing vigilance and multiple layers that address people, process and technology." So says Stephen Orfei, General Manager PCI Security Standards Council.

What are the most common myths around maintaining or achieving the Standard? In my view there are seven.

1. **"PCI DSS compliance is just there to protect the card schemes."** PCI DSS was created by the card schemes in response to Enron. This resulted in the card schemes consolidating their standards and forming the PCI Council to reduce their risk by helping card processers reduce theirs. At the PCI Participating Organisations Conference in Berlin Oct 2014, Stephen Orfei, described the PCI Council's approach to evolving the standard as "*a prioritised risk based approach with the objective of being compliant."* The standard evolves in a structured three year cycle. It will not go away and, through its 12 requirements, provides a structured approach to reducing the impact of organised crime on your company.

2. **"The PCI Council and my acquiring bank are my enemy."** The acquiring bank has to report to the card schemes on all their merchants' progress towards PCI DSS compliance. They get the fines if merchants or card processers do not comply. Since Jan 2015, they have been passing down more of the fines. They are there to help, not to fine you. Communicate openly with them and your QSA (if you have one). It will reduce cost and help you to be secure.

3. **"PCI DSS compliance is not something we should take seriously."** Seriously, compliance is absolutely a board level issue. Ask yourself who it will be in your organisation that faces shareholders, customers and the press if your company has a breach. PCI DSS compliance is about protecting the brand and reputational risk. According to the 2014 Cost of Data Breech study by the Ponemon Institute, fewer customers remained loyal following a data breach. Abnormal churn as a result of the data breach incident increased by eight percent in 2014.

4. **"PCI compliance is a technology thing."** As the PCI Council says, compliance is about "people, process and technology." There is NO silver bullet. There is NOT one single technology solution that will make any organisation PCI DSS compliant.

5. **"PCI is just a compliance project."** In isolation, most businesses are missing opportunities to lower other operational costs. PCI DSS compliance and maintaining compliance, needs to be planned directly alongside the business's overall technology refresh strategy. Separating the two increases costs and increases risk. Having a PCI DSS compliance strategy that takes your organisation out of scope of PCI DSS represents a huge opportunity to significantly reduce both cost and risk. One of the biggest areas of gain is call recording. . For larger merchants, we have seen the opportunity to reduce processing costs.

6. **"PCI compliance is costly."** That depends entirely on how you approach it. Certainly complying with all 12 requirements, irrespective of how many cards your organisation processes has a cost. Complying with Requirement 12 ONLY will absolutely cost less, even in the relatively short term. De-scoping (taking your organisation out of scope of PCI DSS) is absolutely, the best way to go and yes, it has been achieved whilst still allowing the merchant to retain compliant access to their legacy call recording file.
   We have worked with smaller merchants where de-scoping has cost them less than £10K over a five year term.

7. **"De-scoping my contact centre using a DTMF solution is not a great customer experience."** These solutions come in a number of flavours, primarily IVR automated and DTMF control or clamping allowing the agent to maintain voice contact with the customer. Both help de-scope contact centre infrastructure, the later (DTMF control) seeing new engineering offerings with 10 UK providers. Not all are equal by any means. With a growing number of deployments, the evidence from large multi-channel retailers, dealing with customers across a very broad demographic, is very positive. In a recent survey of 1,000 consumers, 60 percent said that they would be more comfortable if they knew that contact centre agents could not hear or access payment card data. (Compliance3 research - Jan 2015).