Information Age Article
February 2015
Version 4 JG sign off

Title suggestions:

- ***"Too many myths, not enough time."***

Subheader:

- ***How the myths of PCI-DSS are holding back 100 per cent compliance.***

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

While PCI DSS is mandatory for any business handling payment cards, compliance is being held back by myths, misinformation and misleading solutions.

The fact of the matter is, credit card fraud is very much still alive and kicking. Hacking data has been well documented, and this is where many PCI DSS solutions focus their attention. However it is the human element of fraud which is causing so much difficulty, and this is where the compliance gap can typically be found. The Financial Fraud Association's 2013 report said, "Chip and Pin fraud is now migrating away from the internet to other card-not-present channels, such as the telephone."

The problem has gotten so out of hand that DCI Mark Wilkie of South Yorkshire Police said, "Call centre internal compromise is the biggest form of up and coming fraud in the UK."

For any business requiring PCI DSS compliance, it's a jungle out there in terms of choosing the right solution. Far too many are making the wrong choice, often leaving them with a partially compliant organisation and a large bill.

The myths of PCI DSS compliance are the root of this problem. As a business that helps UK and multi-national businesses become compliant, we often have to bite our tongue when hearing about the typical Elastoplast fixes that so many businesses implement.

These myths are holding businesses back, and at the same time feeding many organisations that are trying to sell "one size fits all" solutions. Whichever route your business takes, you will need to consider the wider implications of compliance and how it can actually be highly beneficial to your business.

Myth 1. My business needs to store, process or transmit card data.

60% of consumers said that they would be more comfortable if they knew that agents could not hear or access payment card data (Compliance3 research. Jan 2015)

There is not one merchant business in existence that actually needs to manage the storage, processing or transmitting of card data (or what PCI DSS refers to as 'sensitive customer data') themselves, regardless of the industry in which they operate. All these processes can be successfully outsourced thus "de-scoping" all relevant data and data management processes from a business will almost fully remove 11 of the 12 PCI DSS requirements, thus making compliance manageable and affordable from the get-go.

Strangely enough, it is not widely known or acknowledged that a de-scoping PCI DSS compliance strategy will take the burden of compliance away. 100 per cent of businesses can do this, however there are less than 100 businesses in the world that have actually done it and only one that has done it whilst still retaining access to their legacy call recording files that contain card data.

So even businesses that need to access to historical call recordings can still hold no card data within their environment, whilst still meeting their data retention policies and / or fulfilling their FSA obligations. There is an approved way around the legacy call recording issue.

Myth 2. Customer experience will be affected by compliance

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 8 percent in 2014.

While most businesses are focussed on the customer experience, it's no excuse to avoid compliance. The good news is that whilst technology has moved on, so has the consumer – thus modern systems can remove 'personal and financial data from the contact centre environment while still putting the customer first. Sure, there are still people out there that don't want to use the keypad on their telephone or mobile to pay for car parking or a cinema ticket, but customers are much more used to self-service in every form across all age groups and social demographics.

The growing availability of DTMF (Dual-tone multi-frequency) technology vendors (10 now globally, all in the UK) is providing businesses with real and affordable options to reduce the cost of compliance in their contact centres, fully de-scoping telephony, people, desk top, CRM and call recoding.

In addition, automated systems and our understanding of consumer behaviour have taken leaps and bounds over the past five years, and there are affordable systems that will not diminish the customer interface and in many cases satisfy the consumers desire for choice and convenience. These are easy to implement, low costs and very effective solutions.

For example, a top five UK energy provider which has introduced a new and fully compliant automated solution, now successfully completes over 80 per cent of their automated bill payment transactions, where previously it was as low as 20%.

Myth 3. PCI compliance is a technology fix

Ask most businesses, and they will say that PCI DSS compliance has to do with technology. 90 percent of businesses push this responsibility to the IT director where it sits snuggly within the on-going security agenda adding complexity and cost to meet the 12 requirements. They in turn look to their exiting vendors or the vendors operating in this space with the aim of achieving 100 percent

compliance. However, this approach often overlooks the available de-scoping options and there is not one purely technology solution which can provide full compliance on its own. Buying a single technology will not make you compliant.

Why is this? The problem tends to lie in three areas:

1. Some technology solutions (pause resume) do not account for the considerable human risk especially in an open plan office or contact centre. True, implementing a DTMF solution takes people out of scope, but not every tech vendor is equal; they will all give the impression of being 'case hardened' and in a particular way respect industry patents

2. It will de-scope future data, but it does not address the requirement to hold and access legacy data, especially when it is a regulatory requirement (as in the financial services industry)

3. De-scoping reduces cost and risk, but it has to be part of an overall plan, a de-scoping strategy that fully considers people, process and all available technologies

The fact of the matter is that most businesses in the UK are left with partial compliance and a big problem securing people and process. Most businesses in the US are compliant but are left with a high annual cost of maintain compliance and a high risk against people and process (as we have seen with recent high profile breaches)

Myth 4. PCI seen in isolation from the rest of the business

As per the above myth, compliance needs to be integrated with the wider business. 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 can increases risk. One of the biggest areas of gain is call recording, a technology that most larger business deploy to meet either internal or external compliance obligations. For example, an old client

, a large multi channel retailer, had a high end, top brand call recording solution. Their pause / resume was failing. I was leading the deployment of a set of technologies to full de-scope their contact centre estate to help deliver their PCI DSS compliance. , They had just outsourced the management of their contact centres, some were closing, some new ones were opening. Speed and cost were the key drivers to maintain BAU. The solution – to use the DTMF solution vendor to record the calls in their hosted multi-tenanted environment on a site by site basis. The result - site transitions delivered on time, improved agent experience, immediate cost saving circa £1.5M plus ongoing cost saving potential to 'end of life' the high end, site based call recorders.

Myth 5. Management doesn't need to get involved.

PCI risks are bigger than many management teams assume, and any breeches could cripple a business and damage their reputation.

Let's put it this way – if an incident arises where personal card data is stolen or hacked, what will that cost a business in terms of reputational risk, lost business and of course the non-compliant fines which are currently averaging more than $10.8 million. (2014 Cost of Data Breech Study, Ponemon Institute).

Deleted:

Of course, bringing in the right solution in itself is a boardroom issue. In our experience, the boardrooms that take PCI seriously are the ones that can reach 100 per cent compliance and still save money and modernise their infrastructures.

Myth 6. PCI is too expensive.

The way in which compliance solutions are often presented to businesses can lead to this particular myth being perpetuated. Getting the wrong solution and advice can be expensive and detrimental. While there is no quick solution, there are affordable ones. The cost of PCI compliance is also scalable, based on the requirement. As an example, we recently helped a small professional trade association to become compliant, and the whole process cost less then £10k over a three-year period.

Myth 7. The PCI Council and my Acquiring Bank are my enemy.

This is my final myth, and perhaps the most important one to dispel. I attended the PCI Council summit in Berlin last October. It was a fantastic event, well supported by Acquiring Banks, QSA's and other participating organisations and merchants. Every attendee was focused on making things easier for merchants to be secure and protect the value of their businesses.

Stephen Orfei (incoming PCI Council GM) described his future view of the Councils approach to evolving the Standard as "*a prioritised risk based approach with the objective of being compliant.*"

Open and honest communication with your Acquirer makes the businesses task and their task so much easier. Even if the news is not good, it allows them to manage the card scheme expectations. One of our first tasks when assisting a contact centre's PCI challenge is to get the business and their QSA (if they have one) around the table and agree an approach to take to the Acquirer. In all my experiences working with merchants, a problem shared is a problem halved.

In conclusion, it is hard for businesses to get the right operationally led advice on PCI compliance, especially in contact centres. Push it to the IT team, and you will get a purely IT solution. That's why so many businesses in the UK are currently partially compliant and why business in the US have used segmentation to be compliant and in both cases why money and time have been wasted.

Ultimately, PCI compliance is a broader business issue, and if treated this way, the cost of compliance can be minimised and has the potential to be a benefit, not a burden.