Lafferty Group Article
6 May 2015

Word count: 400-500
Deadline: 6 May

The weakest link in PCI-DSS compliance

People are the most vulnerable link in the PCI DSS compliance domain – so what can businesses do to plug the holes?

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

Any firm that processes, stores or transmits payment card data has to meet the Payment Card Industry Data Security Standard (PCI DSS). Compliance to the standard is like a pregnancy. You either are, or you aren't and like pregnancy, fewer are. It's a robust standard that diligently covers all aspects of a firms security, considering people, process and technology, irrespective of a firms size and banded, based on the number of transactions processed per annum. Being compliant is just the beginning of the journey. According to Verizon's 2015 PCI Compliance Report, less than a third (28.6%) of companies were found to be still fully compliant less than a year after successful validation. In addition, research published by The Ponemon Institute for 2014 said that 40% of data breaches involved negligent employees or contractors (a.k.a. human factor) with malicious or criminal attacks increased slightly from 34% percent to 38% percent of data breaches.

This overall position is worrying, especially as consumers tend to be completely unaware of the compliance status of the businesses they are sharing their payment card details with.

Why are so few compliant? In a nutshell, they are looking at the technology, not the people or the process. With very few exceptions, most businesses see PCI DSS compliance as a technology fix and they often see one technology as making them compliant.

"Get the right software in place, and everything will be fine." "Get the IT manager to sort it, they know what they are doing." Common phrases we hear day in and day out which indicate that businesses are ignoring the very weakest of links - the human element involved in the payment process.

How does this manifest?

First off, contact centre agents are exposed to the risk of transgressing to the dark side. The temptation, especially for an individual on a zero hours contract and earning close to the minimum wage, in a harshly managed or oppressive environment, to sell data to a stranger in a car park for £50 per card number and CVV, is simply too real and too much for some people. Firms tend to underestimate this risk, even though the threat is real and well documented. According to Detective Chief Inspector Mark Wilkie of South Yorkshire Police, "Call centre internal compromise is the biggest form of up and coming fraud in the UK." Detective Chief Inspector Derek Robertson of Strathclyde Police stated that "one in ten of Glasgow's financial call centres has been infiltrated by criminal gangs and 100% suffer from criminal fraud."

What is the solution?

Not to expose your people to the risk of accusation. Not to expose your people to the risk of organised crime. Prevent card data from entering your contact centre and implement a solution that allows the customer to enter their sensitive personal data (card data) using the keypad on their phone. Sounds simple? In practice it is, but believe it or not, many firms are either unaware or believe the technology and processes that facilitate this are too expensive. The good news is availability is growing, there is little, or no evidence of the customer thinking this is detrimental to their experience and costs are dropping. .

Whilst we should all be confident that 99.99 per cent of contact centre agents are honest and trustworthy, we just need to take the temptation away from the 0.01 per cent.