



Smart money

You've implemented your quality system, secured your risks

with ISO 27001, got your environmental issues under control, and sweated through your Sarbanes-Oxley (SOx) audits. Can you get any more secure, accurate, green, reliable and compliant? Well, if you process debit or credit card payments, Visa, MasterCard, and other card companies think you can, and they're probably right.

Recent events such as the huge theft of card details from TJX – owners of discount fashion store TK Maxx – show that this concern and need for better control of credit and debit card information is an obvious one. Everyone seems to know someone that has been a victim of a 'cloned' card, and stories of pin-hole cameras and radical terrorist groups lurking in shop cupboards with a laptop hooked into the Electronic Point Of Sale (EPOS) network abound. It has never been easier in this information era to set up an internet business that takes your payment in seconds.

Now, another standard has hit the congested skies of compliance – Payment Card Industry Data Security Standard, or the PCI DSS.

Some years ago, payment card companies started their own individual security standards to try to make merchants and acquirers manage payment information in a secure way. At some point it became obvious to them that they were all effectively asking for the same thing, so they fused it all together and PCI was born.

The PCI DSS 1.1 is defined by the PCI Security Standards Council as 'a set of comprehensive requirements for enhancing payment account data security'. It's mandatory for anyone processing or managing credit or debit card transactions.

The card companies have cleverly placed responsibility for compliance on the acquirers, who in turn need to ensure compliance of their merchants. Fortunately there are four tiers of merchants based on the number of payment transactions processed annually. The major breakpoint is tier one, which is over six million transactions each year. Companies at tier one require an independent audit, where tiers two, three and four are allowed to self assess, though have independent vulnerability scans.

The standard comprises a set of mandatory requirements around the card data itself, and then details 12 compliance chapters consisting of more than 240 controls, covering policy, IT controls, HR and so on. It's a lot like ISO 27001 specifically for card information.

PCI has been around for a few years now, but lack of awareness and effective communication, particularly in the UK, has left many either unaware of its requirement, or baffled by deadlines and potential penalties.

Any good?

As an implementer of ISO 27001, and with an IT technical and security background, I have to say I am cautiously optimistic about PCI. The standard is clear, and because it is targeting a specific set of data and information, the controls are much clearer and more specific than many other standards. There is no ambiguity around storing card information, and the merchant levels for compliance are clear.

The big problem with PCI is communication and clear guidance on implementation. Unlike most other standards, where the ultimate responsibility for the standard and compliance is handed over to independent bodies to audit and certify, the control of requirement and sanction is still held by the card companies. The PCI Standards Council is little more than a librarian, and questions sent their way generally result in being asked to contact the card companies directly.

Deadlines for compliance seem to be in constant flux, and the rules in the US are different to the EU. Some merchants in the UK are getting letters from their banks or acquirers asking for self-assessments, but there is no consistency in the timescales or the specified requirements – ie what if they have areas of non-compliance? Should they supply a remedial action list? Ignore it? No-one currently seems to know, particularly the acquirers. The PCI Standards Council will point you towards the card companies, and different card companies often give conflicting advice.

There are also some technical areas that need clarifying. A lot of companies that process payments usually have call centre environments as part of the sales or customer support processes. One key question recently has been around call recording.

If a transaction is made over the phone, and the three

Payment cards and the internet have radically changed how we pay for products and services. They have also made it easier for theft and fraud to be perpetrated. But, with some prior planning these can be reduced

“Lack of awareness and effective communication, particularly in the UK, has left many either unaware of the standard’s requirement, or baffled by deadlines and potential penalties”

digit security number is requested, recording this conversation breaks PCI rules, as storing of the CV2 number is prohibited. But then many companies use call recording for compliance, quality and even contractual verification. Where does this leave them? Ceasing recording is a major change, and there is no clear guidance on this from the powers that be. The phone system companies are already selling upgrades and bolt-ons to allow pausing of recording, or search and removal of matches to keywords, but these are all at significant additional cost and with no definite guidance yet materialising, companies are unsurprisingly hesitant to rip out and reconfigure their call recording systems.

Another area of confusion is over penalties for non-compliance. Reports from the US are already showing companies receiving fines for non-compliance suggesting amounts such as US\$25,000 (£12,000) a month until compliant. But again, there seems to be differences between US and EU enforcement and sanction.

Recent online and press articles have reported that the card companies will move non-compliant companies onto less favourable tariffs until compliant. The ultimate sanction is removal of the service, though it seems unlikely that the card companies will cut off their revenue streams to spite their face. However, compliance to PCI is a contractual obligation, and litigation on non-compliance could get messy, not to mention action from interested third parties and damage to reputation.

PCI, like many other standards (SOx is a prime example), has no defined requirement for a management system. Implementing controls and standards often ends up in a snapshot of compliance and action at a given time, but then stagnates without a regular plan-do-check-act (PDCA) cycle.

Those with existing certifications to BSI and ISO standards are realising that corporate governance and compliance with standards is a way of life for most companies now, and using management systems to imple-

ment and control these requirements gives them a huge advantage in managing compliance. The real benefit comes in not just scaling the initial peak, but maintaining the requirements. A good management system is often the difference between ticking an audit box, and providing genuine business value.

Use ISO 27001

In particular, anyone that is running an ISO 27001 information security management system (ISMS) should be well-placed to incorporate the predominantly IT and technical-based PCI requirements into their current PDCA processes. There are arguments to say that being certified to ISO 27001 will cover the requirements for PCI.

While this is true for many technical aspects, and an ISMS will get you most of the way, PCI has some mandatory requirements over card data that need to be bolted on. However, it should be an easy process to add the additional controls, and assess the risks in a good ISMS.

Where is it going?

Despite the uncertainty surrounding PCI compliance, one thing is definite – PCI is here to stay, and the clock is definitely ticking. Companies should – if they haven’t already – be assessing their current compliance, and planning for the gaps. Everyone affected should be completing self-assessments demonstrating compliance. Anyone who can show that they take it seriously will undoubtedly find themselves in the right place when the clouds of confusion finally lift.

Most companies I deal with who are affected by PCI are willing participants. They see the value in the standard, and on the whole welcome the clear technical requirements for the card data. No-one wants to be the next TK-MaXX, and no-one wants their name dragged through the media as a result of some breach or non-compliance finding. All they want is some clear advice and guidance on deadlines and penalties

Nick Steele has spent 20 years in IT, with the last five focused on information security. He currently works for Red Island Consulting, specialising in ISO 27001