BIZCOMMUNITY

Reduce scope to ease the pain of PCI compliance

By Peter Harvey

12 Jun 2013

Businesses that process credit card transactions are under increasing pressure to comply with global Payment Card Industry (PCI) security standards - and if our experience at PayGate is anything to go by, the journey is likely to be a painful one. Anybody considering it should prepare themselves for at least two years of intense effort.

We are proud of our PCI compliance certification, and in our business as a payment services provider it's essential to our ability to survive and thrive in the future. But along the way we have had to rethink and redefine the entire way our business is managed, from our IT infrastructure all the way through to our recruitment practices.

Based on what we've learned, if I had one piece of advice to give to anyone embarking on this journey, it would be this: Reduce the scope of the exercise as much as possible.

The need for PCI compliance applies to anyone who transmits, processes or stores full credit card details. So the first thing to do is take a good hard look at how you are using credit card information, and ask yourself if it's really absolutely necessary to your business.

For example, for various historical reasons many systems still use credit card numbers as account numbers. This made sense in the old days - it was a convenient and easy way to identify your customer across multiple systems and different departments, from finance to marketing. But nowadays, when every system is being constantly probed for weaknesses by hackers and organised criminals across the globe, it's a disaster waiting to happen.

Prune right back

There are only two choices in this situation: Either subject your entire organisation to PCI compliance - which I don't recommend - or prune right back to one central card process that you can secure.

This will have knock-on consequences for your CRM systems - but the costs will be much, much lower than PCI compliance.

Your goal should be that your systems should handle credit card information only when it's absolutely necessary and unavoidable. If you can replace a stored card number with a secure token or alias, for example, do it. Tokenisation is a powerful security tool that we're urging more and more of our customers to use.

In fact, if processing card payments is not your core business, there is a strong argument to outsource it to a third party

completely. I believe in the next two to five years we'll see many more companies, including point of sale (POS) system providers, turning over the complex and difficult business of processing card transactions to specialist providers.

If you absolutely can't get away from the need to process, store or transmit card details within your own systems, the first step is to isolate the storage of credit card numbers to one or two systems for which you can provide maximum security. Throw everything you have at it - not just the usual firewalls and anti-virus protection, but also data encryption, intrusion detection and file integrity management. Then have an outside security expert - an "ethical hacker" - test your system for vulnerabilities before you start working on your PCI certification. The insight you gain will be well worth it.

ABOUT PETER HARVEY

Peter Harvey is the MD of PayGate. Leading through integrity, with more than 26 years in IT and payment processing, Peter is a master when it comes to creating solutions to clients' exact requirements. He is a truly integral member of the PayGate team and works tirelessly to ensure its continuing culture of integrity and quality.
View my profile and articles...