PCI Compliance: What Australian Businesses Need to Know

7 June 2009

Most Australian businesses will have recently been contacted by their bank enquiring about their Payment Card Industry (PCI) Data Security Standard (DSS) compliance status. For many organisations this will be the first they have heard about the PCI standard, and are likely to have a few questions: Does this apply to me? What are my obligations? How does this benefit my business?

In brief, all organisations which store, process, or transmit credit card data must comply with the PCI DSS. Whether you accept credit card payments via a website, over the phone, through the mail, or by any other method, compliance is compulsory. The standard is sponsored by the major credit card companies and is developed and administered by the PCI Security Standards Council (PCI SSC). It was developed to help organisations that process card payments prevent credit card fraud, hacking and various other security issues. Failure to comply with PCI can result in heavy fines, restrictions, or even permanent expulsion from card acceptance programs.

The standard requires compliance with 12 broad requirements across 6 control objectives. It is primarily a compilation of security industry best practices which minimise the risk of a security breach or other events which may adversely impact the security of cardholder data. An organisation cannot be partially compliant - i.e. compliance is a pass/fail exercise. Meeting all of the requirements in their entirety can be an onerous task which involves the implementation of security management practices, policies, procedures, a robust network architecture, secure software design and other critical protective measures. Furthermore, there are ongoing obligations to conduct quarterly vulnerability scans and wireless scans, and a requirement for an annual penetration test.

For PCI purposes an organisation will be assigned a merchant level by its bank based on criteria set by each of the card brands. Designation may vary by card brand based on credit card annual transaction volume and/or risk determination. The merchant level assigned will affect whether an organisation can conduct the compliance assessment itself, or whether it needs to engage a Qualified Security Assessor (QSA) to conduct a formal on-site audit. Organisations will often enlist the help of experts in this area regardless due to the complexity of the interpretation of the standard in many areas.

While the standard is developed and maintained by the PCI SSC, it does not run the compliance program. Each of the individual card brands run their own compliance program and as such validation requirements, deadlines, fines and reporting requirements may differ. The compliance deadlines for some card brands, such as Mastercard, have already passed. Other card brand compliance deadlines are later this year or next. Fines of up to US$500,000 per incident can be levied for non-compliant businesses, and there can be other costs including card reissuing and potential civil litigation. Futhermore, a publicised security breach has the potential to negatively impact a company's brand name and reputation.

Aside from the compulsory requirements, being PCI compliant can benefit your business in a number of ways. For example, a company that follows the industry best practices defined in the standard is very unlikely to suffer a security breach. In addition. some organisations use their PCI compliant status to further market their brand to their business partners and customers.

If you have not already considered your PCI compliance obligations it is recommended you start your initiatives as soon as possible. The banks have been actively targeting the higher transaction volume merchant levels for some time, but as most of those organisations are now compliant they have shifted their focus onto the lower levels. Becoming PCI compliant takes most organisations many months, and you should not wait until you receive a letter

from your bank and are faced with increased pressures and deadlines to prove compliance.