

76 Cannon Street
London
EC4N 6AE
02072130999
www.cnsuk.co.uk

The Compliance Journey

Lead Security Consultant
Irfan Iqbal MSc, QSA

5th May 2011

Contents

The Reality	2
The Standard	2
The CNS Journey	3
So what's this all about	3
About the Author	4
About CNS	4

The Reality

As once said by the famous criminal Willie Sutton when asked why he robs banks "that's where the money is". The same motivation is pursued by criminals in the digital age. Merchants, banks and all financial institutions involved in payment processing have become new targets for financial fraud. Poor security, bad practices by merchants have enabled criminals to easily steal and use personal information from payments cards for fraud purposes.

It's a very big problem:

- Between July 2005 and mid-January 2007, a breach of systems at TJX Companies exposed data from more than 45.6 million credit cards.
- In January 2009 Heartland Payment Systems Inc reported a breach within their payment processing systems potentially over 100 million cards being compromised and becoming the largest every breach in history.

The Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a set of comprehensive requirements for enhancing payment account data security. The standard was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. The standard applies to all organisations that **store, process, or transmit** cardholder information from any card branded with the logo of one of the card brands.

The current version of the standard 2.0, was released on 26 October 2010 and specifies 12 requirements for compliance, organized into six logically related groups, which are called "control objectives.

The benefits:

Full compliance to PCI will protect against

- Financial liabilities
- The risk of legal and investigate costs and associated with compromise
- Unwanted public-relation issues arising from compromise

Date

The CNS Journey

CNS has helped many merchants, service providers and financial organisations achieve PCI DSS compliance, by following a simple compliance process.

Scoping: CNS works with the organisation to identify and determine which parts of the business are in scope of the standard. Through interviews, document reviews and network reviews, CNS identifies and analyzes the flow of the cardholder data throughout the organisations network. This includes identifying where data is stored, processed or transmitted. A Mapping exercise is followed up to highlight the systems that have been identified to be in scope.

After determining how cardholder data flows and where it resides, CNS identifies and advises on the most appropriate network segmentation strategy to consolidate where the cardholder data is transacted, processed and stored. This can effectively reduce how much of an organisation's IT environment is truly in-scope for PCI DSS, minimizing the efforts and costs associated with achieving and maintain compliance.

GAP: Once a detailed scoping exercise has been conducted, CNS follows through with the organisation to a GAP Analysis. During this stage, the framework of the PCI DSS Security Audit Procedures v.2.0 will be used. CNS will map the security audit procedures against the organisations current environment, practices and processes. Areas of Non-compliance will be identified and recommendations will be submitted within the GAP Analysis report.

Remediation: Following CNS QSA recommendations the organisation, may wish to work with CNS Solutions team to help remediate any items identified as non-compliant during the GAP process.

CNS QSA work independently from the Solutions team to ensure a rigorous verification can be done to ensure all work carried out by the Solutions team is in line with the PCI DSS standards.

Audit: CNS QSA's will carry out an audit on organisations environment against the PCI security standards to validate the requirements are implemented correctly. At the completing of the audit CNS will complete the Report on

Compliance (ROC) and inform the card brands on the organisations compliance status.

So what's this all about

One of the key mistakes organisations make is they skip or rush the scoping exercise. CNS belief is if that is you nail the scoping exercise on the head the remaining compliance processes will fall into place easily. Many organisations fail to identify ALL the locations where cardholder data is stored and processed on. CNS has found on nearly 90% of organisations they have engaged with; don't even understand why they are storing card data. CNS challenges organisations on their payment processes and storage of card data in every instance to ensure a justified business case is present.

A Success story: ESTATES AND MANAGEMENT (E&M)

CNS was invited by E&M's IT Manager Brian Fraser to undertake on-site PCI DSS scoping exercises as part of its PCI compliance initiative. Being a Level 3 merchant E&M was instructed by their acquiring bank to achieve compliance or face a possible fine. With the threat of fines and no support from the acquiring bank, E&M partnered with CNS to help them with their compliance.

CNS immediately met with the E&M's management to begin the compliance program to prevent any fines being passed on to them.

Immediately CNS identified number issues:

- Cardholder data flow and process had not been mapped and staff were unsure on what was in or out of scope.
- Access to these servers was not controlled correctly.
- Security Policy and Procedures was absent.
- The Internal network was a flat network with no secure segmentation.
- No testing was carried out by third parties to independently verify the robustness of E&M environment internally and externally.

CNS carried out a thorough evaluation and reported back to management on recommendations and immediate actions.

The benefits from Brian Fraser himself:

- **Updating the acquiring Banks:** When E&M was contacted by our acquiring bank, we were unsure what they were asking of us and offered us no real support apart from directing us towards a list of QSA's. We invited CNS to an initial meeting to seek help. CNS broke down the PCI DSS standard, explained how it fits into our business and what was the best approach to take in the most sensible and cost effective manner without compromising security. E&M management found CNS ability to dissect the standard and explain it in a simple fashion was very impressive and we decided that we would partner with CNS.
- **Reducing our scope:** The best thing to happen to E&M was removing certain parts of the network out of scope by isolating departments that processed payments from the remaining network reduced our risk and our compliance scope which in turn reduced the costs and work load for E&M management.
- **Removing card data:** When CNS identified all our systems in scope we were worried we had to spend large amounts of money on solutions and make changes to many of our current business practises. CNS reviewed our current business and payment strategies and worked with the E&M management in exploring different solutions. CNS helped E&M understand their card data flow and map all systems in scope. CNS advised us about the benefits of not storing card data and the impacts it could have had if we went down that road. We understood the complexities of management and cost associated if we had stored card data. Outsourcing this process to a PCI DSS compliant 3rd party payment partner was the correct approach for a small team like ours.
- **Blending PCI into our Business:** Throughout our engagement CNS always asked us how we currently were doing certain business process when it came to security. If they found

E&M had a current process but it didn't quite meet the PCI DSS standards they would try to insert, or get the two processes ensuring the intent of the PCI DSS standard was being met without causing too much disruption. If a process was not in place they would advise on a sensible approach that the business could manage securely.

- **Back to school:** One of the most positive experiences with CNS was the way they educated the whole business from senior management to the desktop user affected by the PCI DSS compliance. It was good to know we were being assisted by people who understood the PCI DSS requirements and our business needs. It gave the E&M IT team the business cases to go to senior management and make changes and implement practises otherwise would have been difficult to implement before.
- **Achieving Compliance:** I am glad E&M chose CNS as partner, their knowledge, experience, and business acumen helped us achieve compliance in a cost effective, pragmatic and secure manner. CNS made this PCI DSS journey an educational and pleasant experience.

About the Author

Irfan Iqbal has been a QSA and Security Consultant at CNS. He has over 5 years experience within the QSA industry working with Banks, Service Providers and Merchants.

Irfan's specialist areas include secure network design, implementation, development and compliance, these include.

- Secure infrastructure builds for compliance and regulation i.e. Payment Card industry (PCI) and ISO27001.
- Programme management.
- Risk Management
- Policy/Standards/Guidelines/Procedures/Methologies Development and Deployment.

About CNS

CNS is a specialist security and networking consultancy, established in the City of London in 1999. CNS has built an excellent reputation for information security and networking consultancy & services to our customers across a variety of sectors on a global scale.

CNS has three delivery divisions as follows:

- Network & Security Solutions
- Security Assessment
- Managed Services