

## **Estates & Management achieve PCI Compliance with the help of CNS**

*CNS counsel and services ease the journey for merchant compliance.*

### **Situation**

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 was being stored in a number of areas with no real business justification to support it. The website was storing card data on the internal servers for no particular business reason.
- 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.

### **Solution**

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. An example would be how CNS advised E&M to stop storing card data on internal systems within E&M and outsource this to a PCI DSS complaint 3<sup>rd</sup> party payment processor. This dramatically changed our compliance status, reduced the costs in implementing solutions to protect card data and reduced the work load 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 gel 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 CNS

CNS is a specialist IT security and networking consultancy, established in the City of London in 1999. CNS has been a PCI QSA for over 5 years. The company is wholly owned by its employees and directors. 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's customers vary in size from FTSE 100 and large public sector organisations to SMEs, but are united in the importance of digital information to their business and in



**working together with our tenants**

their desire for pragmatic, knowledgeable help in securing their systems and data and meeting their connectivity requirements.