Abstract

The explosion in internet usage in the past twenty years has resulted in a significant rise in e-commerce. E-commerce is characterised by the buying and selling of goods and services using computer networks. With the significant growth in e-commerce sites like “Amazon.com”, “eBay.com” and “Alibaba.com” (retail sites), Paddypower.com (bookmaking site) or Priceline.com (travel site) there has been a significant increase in payment card transactions. This has resulted in an increase in attempted fraud. The Payment Card Industry “PCI” has attempted to maintain credibility in e-commerce payments by requiring all e-commerce sites, who accept payment cards, to be compliant with the Payment Card Industry Data Security Standard or “PCI DSS”. Despite the requirement for all e-commerce sites who accept payment cards to be compliant with the PCI DSS, levels of compliance continue to be low. Semi-structured interviews, with participants from across the PCI, were conducted to gain an understanding of why there continues to be a low level of compliance with the PCI DSS. The study concludes that the PCI DSS is regarded as a comprehensive Information Security standard which reduces the potential for a security breach. Organisations only adopt the standard if required to do so by their acquirer or a customer. The degree of adoption is dependent on the Information Security culture of the organisation. Those organisations with a strong Information Security culture adopt the standard broadly across all IT systems. Those organisations with a weaker Information Security culture implement the minimum requirements of the standard. There are several key factors which influence the adoption of the standard. The PCI DSS is costly to implement and maintain. The PCI DSS contains complex language and there is a need for dedicated IT staff to ensure compliance is maintained. Senior executives are more concerned about damage to their brand than concerned about fines from the PCI DSS. As the PCI DSS is managed by the acquirers, commercial factors may result in low levels of compliance. As PCI auditors are employed by the merchant, commercial factors may also impact levels of compliance. There are several recommendations resulting from this research. Tthe PCI DSS should be managed by the PCI SSC and not by acquirers. QSAs should be limited to providing a single service to a merchant. Assessment of the PCI DSS should be undertaken quarterly. Data breach notification should be mandatory. The PCI DSS should be a legal requirement for all organisations who wish to process card data.

Keywords

PCI, credit card, e-commerce, security, cyber security, standards compliance