PCI DSS

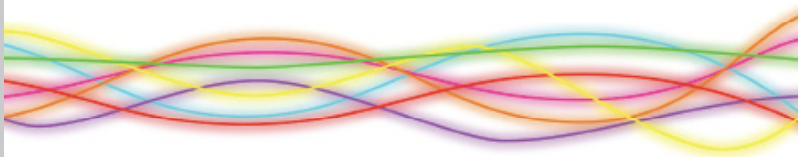
Building Customer Loyalty through Increasing Customer Trust

The Payment Card Industry Data Security Standard (PCI DSS) is a set of baseline technical and operational requirements designed to prevent the compromise of cardholder data. It applies to all entities that store, process or transmit cardholder data and is designed to encourage and enhance cardholder data security through the adoption of consistent data security measures.

It's the consistency that is key – complying with the DSS is not a matter of bureaucracy but a proven methodology that acts as both a deterrent and a defence against malicious attacks. In fact, the latest Verizon 2012 Data Breach Investigations Report showed that in 96% of the breach cases they investigated, the customer was not compliant with the PCI DSS.

Consequently, merchants who fail to comply with the PCI DSS place both themselves and their customers at unnecessary risk, and there are strict penalties in place to enforce compliance. For example, VISA Europe can impose a minimum fine of €26,250 on organisations that do not confirm compliance status within 120 days of notification, with an additional €26,250 accruing for every 30 days thereafter. Other cards have not published the fines they impose, and elsewhere they may be significantly higher. These fines along with the potential for increased fees or withdrawal of licence are passed down to the merchant through their acquiring bank with increasing penalties the longer a merchant is unable to report their compliance status.

Of course, when cardholder data is compromised, the fines become much more significant, as do the more long term ramifications surrounding reputational damage and brand impact. This was the case with TJX, parent company of discount stores T.K. Maxx, T.J. Maxx and Marshalls, who in 2007 disclosed that information on possibly tens of millions of credit and debit cards had been stolen. Though at first the security



leak was supposed to have been vulnerable for around 8 months, it later emerged that the security flaw had been present for almost a year longer than that. All in all, the incident cost TJX millions of dollars in fines and remunerations paid to the FTC (Federal Trade Commission), credit card companies, banks, and consumers. In 2011, Sony PlayStation admitted a huge breach in its video game online network. The name, address, date of birth and potentially the credit card details of up to 77 million users had been stolen in what is believed to be one of the biggest-ever online data breaches damaging the company financially as well as impacting their reputation and brand.

Meeting PCI DSS

So, any entity that stores, processes or transmits cardholder data needs to prove compliance with the PCI DSS standard and the requirements of the standard apply to all system components that are included in or connected to the cardholder data environment. Consequently, there are challenges in meeting both the technical and procedural requirements of the standard.

The number and type of those requirements depends on how card processing takes place. How an organisation reports and proves compliance against those requirements then depends on the volumes of card transactions the organisation handles on an annual basis.

The requirements of the PCI DSS vary from securing card holder data at rest and in transit to physical security and on-going monitoring and there are many approaches that can be adopted to address these requirements.

2e2's PCI DSS Qualified Security Assessors (QSAs) can work with an organisation at any stage of its' PCI compliance lifecycle. For instance, the initial scoping exercise and gap analysis help identify appropriate remediation and provide recommendations on segregation to reduce the scope of compliance.

Additionally, we can perform on-site assessments for initial compliance or offer recommendations for how the organisation can maintain compliance over the course of their annual audit cycle.

Changes to Self Assessment Questionnaires

Where previously organisations could complete self-assessment questionnaires (SAQs) uninhibited, Mastercard recently announced that from 30th June 2012 all of their Level 2 customers must ensure that the relevant staff attend PCI SSC ISA Training and pass the associated accreditation programme annually in order to be eligible for self-assessment compliance validation. With a customer base as large as Mastercard's, these new measures effectively apply to all level 2 merchants, meaning huge numbers of internal staff now require further training.

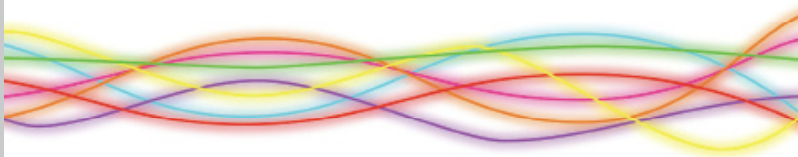
Alternatively, Level 2 merchants may, at their own discretion, complete an annual onsite assessment conducted by a PCI SSC approved QSA. 2e2's Security practice can provide PCI DSS QSAs to conduct the onsite annual assessments.

Whichever option is chosen, level 2 merchants must adapt to significant changes in the compliance attainment process.

Why 2e2?

Before an organisation can know what controls to implement, it is necessary to understand the scope of where an organisation's card holder data exists. By understanding the scope, options for minimising the scope through network segmentation or tokenization techniques can be investigated. This ensures that the requirements of PCI DSS need only be applied to the relevant systems.

Firstly a data discovery activity should be undertaken. Only once an organisation fully understands where its cardholder data resides can it then look at reducing the scope of works by removing cardholder data from where it's not needed.



Once the scope is understood a gap analysis exercise will help the customer understand the remediation controls they will need to implement. Based on these remediation recommendations 2e2 can provide an action plan based around the PCI DSS Prioritised Approach which will help customers to report to their banks on their progress towards compliance.

Along with remediation recommendations on how the customer can address compliance drivers, 2e2's other technology divisions can assist with the implementation of various technical controls to meet those requirements. Additionally through the 2e2 Security practice, assistance can be provided on developing and implementing the relevant procedural and policy requirements. For example 2e2 can assist with developing and implementing security awareness training as required by the PCI DSS standard, or draft or amend existing policies to ensure they align with the PCI DSS requirements.

2e2's Security practice also provides PCI DSS QSAs who can then undertake the audit and assessment activities necessary to report on compliance.

Additional advice can be provided for maintaining on-going compliance. The assessment process is a point-in-time audit but organisations must maintain compliance throughout the annual assessment period. This includes activities such as quarterly external vulnerability assessments conducted by qualified PCI Approved Scanning Vendors (ASVs). 2e2 partner with ASV companies to conduct these scans and advise on remediation required to maintain "passing" scans.

Furthermore, 2e2 can deliver the required bi-annual review of firewall rule sets or conduct internal network vulnerability assessments. The 2e2 Security practice offers information assurance professionals who advise on or conduct annual risk assessments using formal methodologies appropriate to the size of the organisation.

For more information, please contact:

a. The Mansion House
Benham Valence
Speen
Newbury
Berks RG20 8LU

t. +44 (0) 8442 250526
e. info@2e2.com
w. www.2e2.com