

## Straight Talking - PCI-DSS: Why compliance with this card security standard adds up

By Bob Tarzey, Service Director, Quocirca Ltd

The Payment Card Industry Data Security Standard (PCI-DSS) is now more or less mandatory for any organisation handling payment card data. It is hard to be categorical about compliance because the PCI Security Standard Council (PCI-SSC), the body that oversees PCI-DSS, does not itself mandate compliance. That responsibility falls to the five main payment card brands that oversee the standard: American Express, MasterCard, Visa, Discover and JCB International.

The demand from the brands for compliance varies by geography and business size, as measured through the number of payment card transactions processed per year. But there are now few areas where PCI-DSS is not compulsory for any businesses wanting to process payment card data. Even businesses that process just one transaction are expected to comply.

The reason PCI-DSS compliance has become a pressing concern is the degree to which payment card data has become the target of fraud. London-based consultancy 7Safe indicates that 85 per cent of all sensitive data breaches involve payment card data.

The PCI-SSC is increasingly concerned with protecting the business of its members and maintaining the confidence of the service providers, merchants and consumers that rely on payment cards.

Failure to comply can be costly, especially if a breach occurs. Penalties could be levied at three levels. First, for non-compliance by one or more of the card brands. Second, for the breach itself. Third, if the leaking of payment card data is part of a broader data loss event, there could be fines from other regulators, including the Information Commissioner's Office and the Financial Services Authority.

Covering up breaches is also not acceptable. For example, the Rules for Visa Merchants say any

business that handles payment card data should have a clear written policy in place, detailing procedures for handling payment card data and suspected breaches.

Should a breach occur, the rules state you should contact the police, the bank and Visa fraud control, as well as preserve all logs. In other words, disclosure is mandatory as part of the agreement to handle Visa transactions in the first place. Other brands have similar requirements.

The best thing of course is to avoid breaches altogether and that is what PCI-DSS is all about. At the top level, the standard "strongly discourages the storage of cardholder data". If you do not store it, you cannot lose it.

For small businesses that rely on cardholder-present point-of-sales devices this is pragmatic advice. But for businesses that rely on transacting online or over-the-telephone payments, many want to collect and store payment card data to handle repeat business or refunds without referring back to the cardholder.

Storage is strictly limited to just four data items that are sufficient to handle these requirements; the primary account number, or PAN, card holder name, expiry data and service code, a part of the magnetic strip data. You are explicitly not allowed to store CVV2/CID code - for example, the three numbers on the back of a Visa card - full magnetic stripe data or account holder PINs.

If you do store such details then you need to meet the 12 security requirements of the PCI-DSS standard and the 234 sub-requirements that fall under them. The list is too long to repeat here, but the standard can be downloaded for free from the PCI-DSS website.

Suffice to say it covers all aspects of good security practice from maintaining a secure

network through encrypting sensitive data and secure access management to making sure online applications are free of vulnerabilities.

Proving compliance requires an assessment by a qualified security assessor for organisations processing over six million transactions a year, at least for Visa, and for organisations processing fewer than this, the completion of a self-assessment questionnaire. It also requires that most organisations undergo a quarterly network scan by an approved scanning vendor as well as completing an attestation of compliance form.

According to VeriSign, the most common reasons for failing an audit are: data on unsecured physical assets, such as tapes and PCs; PoS application vulnerabilities, such as devices that are not fully behind the firewall being used to store payment card data; unencrypted spread sheets; poorly designed networks with payment card data in open stores; and a lack of log monitoring.

This information might sound a lot to take on at once if compliance has not been considered before. However, the PCI-SSC is pragmatic. It accepts that not all measures can be achieved at once, so it suggests six steps to compliance:

- Remove sensitive authentication data and limit retention.
- Protect the perimeter, internal and wireless networks.
- Secure PC applications.
- Monitor and control access to systems.
- Protect stored cardholder data.
- Finalise milestone requirements.

As long as a roadmap to compliance is agreed, then overnight compliance is not required, but a breach is still a breach and that could still lead to consequent penalties. As the PCI-DSS points out, even compliance does not guarantee security.

Being compliant makes sense. The standard is as good a starting point as any for reviewing IT security. Its requirements are similar to other data security standards such as ISO27001. Recent research included in the Quocirca You sent what? report shows that most businesses expect regulations to increase in a number of areas. The report recommends adopting a "compliance-oriented architecture" to be able to keep on top of existing and new regulations that affect the way all sensitive data is handled and stored.

Those who deal with payment card data are dealing with the most sought-after type of data. Such data is compromised at the guilty organisation's peril.

## About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at

<http://www.quocirca.com>