

## CRN – Data security a lucrative market

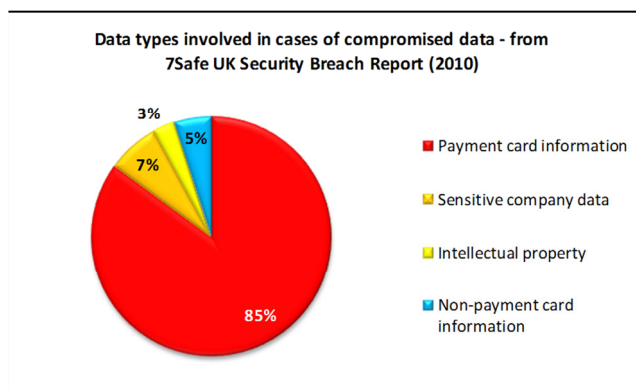
By Bob Tarzey, Analyst and Director, Quocirca Ltd

The increasingly important Payment Card Industry Data Security Standard (PCI-DSS) means there are services that any business of any size which processes payment card data will require, and that there is more motivation for IT security spending in general.

The standard is now more or less compulsory, even though the PCI Security Standard Council (PCI-SSC) does not itself mandate compliance. That is down to the five main card brands that oversee the standard: American Express, MasterCard, Visa, Discover and JCB International.

Payment card data has increasingly been targeted by fraud (fig 1). And failure to comply with the standard can be costly, especially if a breach actually occurs. Penalties may be levied for non-compliance by one or more of the card brands, for the breach itself, and -- if the leaking of payment card data is part of a broader data loss event -- as fines from other regulators.

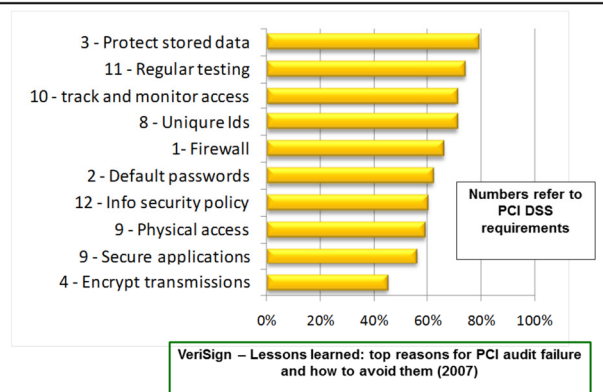
Figure 1: The appeal of card data



The best thing of course is to avoid breaches altogether. At the top level, the standard 'strongly discourages the storage of cardholder data'. However, businesses that rely on transacting online or over the telephone payments, may want to collect and store payment card data, to handle repeat business or

refunds without referring back to the card holder.

Figure 2: Top reasons for audit failure



You are only allowed to store the four data items sufficient to handle these requirements: the primary account number (PAN), card holder name, expiry date and service code (a part of the magnetic strip data). You are expressly not allowed to store CVV2/CID code, full magnetic strip data or account holder PINs.

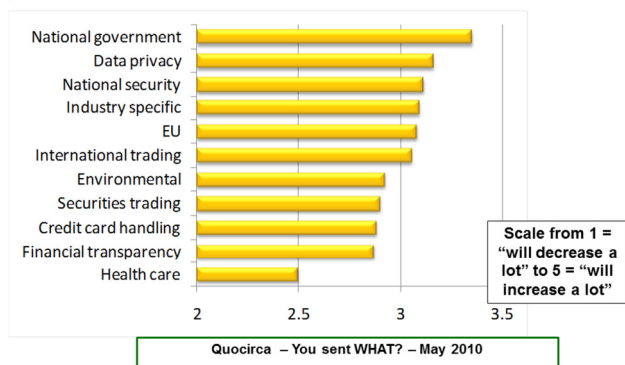
If you do store such data, you need to meet the 12 security requirements of the PCI-DSS standard -- and the 234 sub-requirements that fall under them. The list is too long to repeat here, but the standard can be downloaded for free from the PCI-DSS web site. It covers all aspects of good security practice.

Proving compliance requires the services of a qualified security assessor (QSA) for organisations processing over six million transactions a year. For organisations processing fewer transactions, a self-assessment questionnaire (SAQ) must be completed. Most must also undergo a quarterly network scan by an approved scanning vendor (ASV) as well as completing an attestation-of-compliance form.

Any reseller could apply to become a QSA and offer assessment services to its customers. Verisign recently laid out what it believes are the

most common reasons for audit failure (see the chart below). Identifying and fixing such problems is another opportunity for resellers.

**Figure 3: How do you see regulations in the following areas affecting your organisation over the next 5 years?**



The PCI-SSC and card brands accept compliance cannot be achieved overnight and will allow the continued processing of data if a roadmap to compliance is in place. Resellers that understand PCI-DSS can help their customers do this.

Compliance makes sense. The PCI-DSS requirements are similar to other data security standards, such as ISO27001. Our recent research shows that most businesses expect regulations to increase in a number of areas (figure 3). Payment card data is not top of the list, but that is because it is not essential for all businesses.

For those that do deal with payment card data, the PCI-DSS is as good a starting point as any for compliance-oriented architecture (COA) -- a central recommendation of the report. Payment card data is highly attractive to fraudsters. Organisations that leak it do so at their 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>