

e-finance&payments law&policy

FEATURED ARTICLE
06/08



cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

PCI DSS compliance: challenges to implementation

A survey conducted on behalf of NetIQ reveals how far companies have progressed with implementing the Payment Cards Industry's Data Security Standard since the compliance deadline at the end of 2007. Geoff Webb, Senior Manager of Product Marketing at NetIQ, details the challenges to implementation that companies have faced, their perception of the benefits of compliance as compared to the actual benefits, as well as the penalties available for non-compliance.

Few industries rely more completely on trust than the payment card industry (PCI). The ability to securely and reliably use a credit card to make purchases, especially over the internet, has become a staple of twenty-first century commerce. And yet a series of dramatic and extensive data thefts, most notoriously the TJX theft of over 90 million customer records, is eroding the public's confidence in how safely their personal information is stored.

It was to avert such fears and ensure the long-term trust of the cardholding public that card issuing companies such as MasterCard, Visa, American Express and others, formalised the PCI Data Security Standard (PCI DSS). The Standard is composed of twelve broad sets of requirements designed to make certain that organisations adhere to specific security practices surrounding sensitive cardholder data.

At its core, the PCI DSS was created to protect the kinds of credit card information that are, unfortunately, the target of data thieves operating around the globe. Everything from anti-virus programs to segregation of duties is covered in the Standard in order to reduce the risks to customer data, and while many of the security controls required already exist in most organisations, some technologies are either very new or far more extensive than their predecessors.

Implemented fully, these controls outlined by the PCI DSS should provide a highly secure environment within which credit card information is secured, encrypted, protected from malicious attack and constantly monitored. In short, it is the kind of comprehensive protection that consumers demand for their sensitive, in-demand information.

While this Standard seems like an

ideal approach to securing this critical data, recent studies of PCI DSS implementation show that for many, meeting even the minimum requirements has been far from easy. A survey conducted this year on behalf of NetIQ Corporation, a global Systems and Security Management solutions provider, compiled data from over 500 organisations across the UK and North America that are directly impacted by the PCI DSS. The survey results demonstrate that while the specific compliance challenges between North American and UK-based businesses varied, there were some common trends that may signify similar storm clouds on the security horizon.

When asked how long they had been working on achieving PCI DSS compliance, a surprising number indicated that they had only just begun. In the UK, approximately 25% had been working on building the compliance programs for a month or less - despite the fact that the PCI DSS was launched in 2005 and the last deadline for compliance passed at the end of 2007.

Those only now beginning to work on compliance are likely to have a long road ahead. Almost half of those surveyed in the UK and around two-thirds in North America said that they have been working toward PCI DSS compliance for more than six months, and indeed other related industry research confirms that typical implementation times are between 12 and 18 months in total.

More surprising is that less than one quarter of companies indicated they were currently compliant with the PCI DSS, and approximately half (both in the UK and the US) said they were unable to gauge when they would reach the necessary security levels required for certification.

Why are so many companies unable to even estimate when they can hope to achieve compliance, and for those that can, why is it taking so long? Part of the reason may be that the changes required to become sufficiently secure are extensive and in many cases, these changes affect business-critical systems and applications, making adherence to the PCI DSS a daunting task for many organisations. The day-to-day business operational requirements simply overwhelm the organisation's best intentions to meet their compliance goals.

Additionally, many companies simply lack the basic policy guidelines or expertise to decide how to implement the goals specified in the PCI DSS. In many cases, this lack of good policy around card holder security directly impedes implementation, leaving systems vulnerable and at risk of security breaches.

The difficulties around complying with PCI DSS were reported in a June 2007 Aberdeen Group report¹, in which it was shown that the total cost of PCI compliance was between 1.4 and 3.5 times more than companies had typically estimated. As organisations come up against the steep PCI DSS requirements and expend more resources than expected, they are often tempted to slow implementation, procrastination or simply shelving the program entirely.

While difficulties and cost are clearly having an impact, another factor may be contributing to the poor adoption rate of the PCI DSS. One of the most obvious drivers to achieve compliance is the risk that non-compliant vendors will be penalised by the card issuing organisations such as Visa or MasterCard. Theoretically, such penalties may include significant fines measured in hundreds of

Those only now beginning to work on compliance are likely to have a long road ahead

thousands of dollars or pounds sterling for each incident of non-compliance. However, when asked whether they felt that fines would actually be levied against non-compliant companies (especially so-called 'Level One' vendors, the largest handlers of credit card data), most organisations surveyed replied that such fines would apply only 'occasionally'. Indeed, over 70% of UK organisations felt this way.

Roughly half of the businesses surveyed also felt that becoming compliant would only actually render their data 'slightly more secure'. Not exactly a rousing endorsement.

With businesses feeling they have little to gain from compliance, and less to lose from non-compliance, is it any wonder that they regard the whole process with a degree of weary cynicism? The fact is, however, that these organisations may simply have it wrong.

Vigorous enforcement is becoming increasingly likely. Fraud is now one of the most significant problems facing organisations, most importantly fraud or theft perpetrated by people with inside access to sensitive data. As a result, the credit card companies are starting to feel the financial pain to such a degree that ever more stringent enforcement of security standards is now inevitable. In 2006, Visa levied approximately \$4.6 million in fines, and while it may seem that breaches occur with distressing regularity, Gartner, Inc. reports that only 11% of incidents are ever made public². It is evident that breaches are more widespread than anticipated, and growing in scope and frequency.

It's not all bad news, though. Many of the organisations that approached PCI DSS compliance in a systematic and proactive way are already seeing unexpected benefits associated with their

compliance programs.

The most significant are:

- Better security around sensitive data (not just credit card information).
- Lower risk of non-compliance.
- Better ability to meet future compliance goals.
- More efficient business processes.

While a number of organisations have reported only a slight increase in credit card security, those who have taken the most aggressive approach to PCI DSS compliance have seen far more significant results in their ability to protect sensitive data of all kinds. For these organisations, adherence to the PCI DSS has enabled them to more easily achieve compliance with other regulations, thus saving them additional time and money. Furthermore, with its heavy focus on securing sensitive data, the PCI DSS is now being seen by security professionals as a likely foundation for future sets of compliance requirements. As a result, those businesses that readily adopted the best practices embodied in PCI DSS are also likely to be ideally positioned to meet new regulations and drive more efficient processes for handling sensitive corporate data in the future.

One of the key emergent areas of security technology that may help many of the sceptics adopt and achieve PCI DSS compliance at lower cost is IT Process Automation - that is, the automation of the mundane, repetitive security tasks often demanded for compliance purposes.

While most people would assume that computer systems are generally automated as is, the reality is that business processes, especially those around security, are often very dependent on manual intervention.

The ability to automate the

processes around PCI DSS compliance management, especially detecting and reacting to potential security breaches, will provide organisations with a number of benefits. Specifically, automated security and compliance programs:

- Are cheaper as they require less expensive human intervention.
- Provide better security because reaction to attacks occurs more systematically and rapidly than when it relies on often overworked security staff.
- Are more streamlined, meaning that they not only cost less, but can be re-used or expanded as necessary with business and policy changes.
- Provide a faster path to compliance, especially for future or changing regulations.

So while PCI DSS compliance has proven to be a challenge for most organisations, automating the security processes around credit card data protection holds the promise of increasing security while reducing the overall costs.

There is now little debate that the PCI DSS represents an important step in ensuring the security of consumers' credit card information, and this Standard has become an equally important element of maintaining trust in the payment card industry. Although organisations on both sides of the Atlantic are reporting short-term pain and difficulty in becoming compliant, early adopters are reporting favourable results from their efforts. While the last deadline for compliance passed in 2007, it is evident that the PCI DSS story is far from over.

No one could have foreseen just how the PCI DSS would impact the market, or just how difficult weathering the subsequent sea change would be. But, all indicators suggest that persistence and good planning will reward

those who take a comprehensive approach. Such approaches become more effective and compelling when coupled with emerging IT developments that offer the promise of a simpler, less expensive road to PCI DSS compliance with the added benefit of more streamlined business processes and improved security.

Then, perhaps, we consumers will be the ones left holding all the cards.

Geoff Webb

Senior Manager of Product Marketing
NetIQ

geoff.webb@netiq.com

1. 'Protecting Cardholder Data' - Aberdeen Group, June 2007.
2. 'PCI Data Security Standard: Nothing Left to Comply With by 2018' - Avivah Litan, Gartner Inc., 2008.



cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Registered number 2676976 Registered address 141 Wardour Street, London W1F 0UT VAT registration 577806103

e-commerce law & policy

Many leading companies, including Amazon, BT, eBay, FSA, Orange, Vodafone, Standard Life, and Microsoft have subscribed to ECLP to aid them in solving the business and legal issues they face online.

ECLP, was nominated in 2000 and again in 2004 for the British & Irish Association of Law Librarian's Legal Publication of the Year.

A twelve month subscription is £420 (overseas £440) for twelve issues and includes single user access to our online database.

e-commerce law reports

You can now find in one place all the key cases, with analysis and comment, that affect online, mobile and interactive business. ECLR tracks cases and regulatory adjudications from around the world.

Leading organisations, including Clifford Chance, Herbert Smith, Baker & McKenzie, Hammonds, Coudert Brothers, Orange and Royal Mail are subscribers.

A twelve month subscription is £420 (overseas £440) for six issues and includes single user access to our online database.

data protection law & policy

You can now find in one place the most practical analysis, and advice, on how to address the many problems - and some opportunities - thrown up by data protection and freedom of information legislation.

DPLP's monthly reports update an online archive, which is an invaluable research tool for all those who are involved in data protection. Data acquisition, SMS marketing, subject access, Freedom of Information, data retention, use of CCTV, data sharing and data transfer abroad are all subjects that have featured recently. Leading organisations, including the Office of the Information Commissioner, Allen & Overy, Hammonds, Lovells, BT, Orange, West Berkshire Council, McCann Fitzgerald, Devon County Council and Experian are subscribers.

A twelve month subscription is £390 (public sector £285, overseas £410) for twelve issues and includes single user access to our online database.

world online gambling law report

You can now find in one place analysis of the key legal, financial and regulatory issues facing all those involved in online gambling and practical advice on how to address them. The monthly reports update an online archive, which is an invaluable research tool for all those involved in online gambling.

Poker, payment systems, white labelling, jurisdiction, betting exchanges, regulation, testing, interactive TV and mobile gaming are all subjects that have featured in WOGLR recently.

Leading organisations, including Ladbrokes, William Hill, Coral, Sportingbet, BskyB, DCMS, PMU, Orange and Clifford Chance are subscribers.

A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.

world sports law report

WSLR tracks the latest developments from insolvency rules in football, to EU Competition policy on the sale of media rights, to doping and probity. The monthly reports update an online archive, which is an invaluable research tool for all involved in sport.

Database rights, sponsorship, guerilla marketing, the Court of Arbitration in Sport, sports agents, image rights, jurisdiction, domain names, ticketing and privacy are subjects that have featured in WSLR recently.

Leading organisations, including the England & Wales Cricket Board, the British Horse Board, Hammonds, Fladgate Fielder, Clarke Willmott and Skadden Arps Meagre & Flom are subscribers.

A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.

- Please enrol me as a subscriber to **e-commerce law & policy** at £420 (overseas £440)
- Please enrol me as a subscriber to **e-commerce law reports** at £320 (overseas £440)
- Please enrol me as a subscriber to **data protection law & policy** at £390 (public sector £285, overseas £410)
- Please enrol me as a subscriber to **world online gambling law report** at £520 (overseas £540)
- Please enrol me as a subscriber to **world sports law report** at £520 (overseas £540)

All subscriptions last for one year. You will be contacted at the end of that period to renew your subscription.

Name

Job Title

Department Company

Address

Address

City State

Country Postcode

Telephone Fax

Email

1 Please **invoice me** Purchase order number

Signature Date

2 I enclose a **cheque** for the amount of

made payable to 'Cecile Park Publishing Limited'

3 Please debit my **credit card** VISA MASTERCARD

Card No. Expiry Date

Signature Date

VAT No. (if ordering from an EC country)

Periodically we may allow companies, whose products or services might be of interest, to send you information. Please tick here if you would like to hear from other companies about products or services that may add value to your subscription.

priority order form

FAX +44 (0)20 7729 6093

CALL +44 (0)20 7012 1380

EMAIL dan.towse@e-comlaw.com

ONLINE www.e-comlaw.com

POST Cecile Park Publishing 17 The Timber Yard, Drysdale Street, London N1 6ND