

## THE CORPORATE IT FORUM

Subscribers to The Corporate IT Forum have access to an enormous network of corporate IT professionals and skills in a wide range of diverse organisations across Europe.

Available to subscribers is a wealthy bank of knowledge to which everyone makes significant contributions and unlimited withdrawals of experience through a range of activities including over 60 free workshops, without IT suppliers.

There are NO supplier sales pitches or IT Consultants.

You can find out more about The Corporate IT Forum, forthcoming workshops, and the vast range of information available to subscribers by contacting Lisa Mullins on 01442 866634 [lmullins@tif.co.uk](mailto:lmullins@tif.co.uk) or visit the website [www.tif.co.uk](http://www.tif.co.uk).

## Delegate Organisations

35 delegates attended from 27 organisations affected by PCI. Delegates came from large international retailers, government, local government and the financial services sector.

## Agenda Topics

The workshop delegates received presentations from Visa and were allowed to submit feedback directly to the company. They also received a presentation from QSA AmbironTrustWave. Other agenda items included a discussion around audit and network scanning experiences, global compliance issues, reporting and communications issues.

## Workshop Process

This is the third in a series of workshops designed to assist subscribers to resolve their issues around PCI compliance.

## Summary

Subscribers are in favour of the Standard, they are aware of the benefits and are keen to comply.

Implementation is the major problem. Delegates called the situation: *“chaos”, “bad business and bad management”, “appalling”, “a total mess”*.

Confusion still exists and subscribers still feel “left in the dark” due to poor chains of communication between card schemes, acquirers who are supposed to pass information on (but often don’t) to the end merchant.

Different approaches to compliance exist between the card schemes, MasterCard and Visa, with MasterCard imposing a fixed compliance deadline of June 30 2007 and Visa having a more flexible approach – but to the same set of Standards. Visa’s approach appreciates the difficulties merchants have with compliance and only requires merchants only to ‘show intent’ of compliance – although there is still lack of clarity around what this means and for how long it will be sufficient to ‘show intent’.

There still remains a lack of consistency between different acquirers and card schemes:

There is a total lack of understanding from the Card Schemes that businesses need clear and unambiguous information in order for them to go to their board and ask for the budget needed to implement PCI. There is confusion around what can happen legally if they don’t comply.

People have found out about PCI 'by accident' (through media, other subscribers etc) and are continuing to do so.

There are huge differences between the levels of compliance and awareness between different organisations. Some (but very few) subscribers are now compliant, others have just found out, others have found out but are unsure as to what to do. Some people are aware about the need to contact a Qualified Security Assessor (QSA) to audit compliance, others didn't know what a QSA was.

There are around 20 to 30 QSAs across Europe who will need to assess every merchant across Europe – many are worried that this is too few.

Some budget has been spent by Visa on building awareness within the acquirer and merchant community of PCI but many see this as being "too little too late".

Subscribers feel that they are "going round in circles". When questions are relayed back the acquirers regarding timescales and deadlines (as instructed to do so by the card schemes), acquirers either do little with the request, or pass the questions back to the card schemes – which then don't get answered.

In many cases, the technical expertise doesn't appear to exist within the acquirers to deal with merchant's questions.

## Contents of the Full Report

The following is a list of the additional material contained in the full output report from PCI Compliance: The Next Steps Workshop. Subscribers can download any of the 200 workshop output reports via the website. Non subscribers will receive the full output report (circa 15 pages) from the workshop that they attended for which the full fee of £375 has been paid.

- Summary and Best Practice Conclusions
- Presentation by Visa
- Visa Presentation Q&A
- Presentation by AmbironTrustWave (ATW)
- ATW Presentation Q&A
- Audit & Network Scan Experiences
- Global Compliance Issues
- Reporting & Communications Issues
- Post Workshop Discussion Q&A
- Learning points
- Related Links
- Actions
- Delegate List

**Disclaimer:** The views and opinions expressed herein do not necessarily reflect the views held by subscribers to The Corporate IT Forum neither does The Corporate IT Forum Ltd accept responsibility for the correctness or consequences of following any of the suggestions expressed herein.