

THE CORPORATE IT FORUM

The Corporate IT Forum Service (commonly referred to as tif.) was initiated by a group of the largest corporate users of IT. The group wanted to share and exchange information about delivering better value from corporate IT and to learn from each other in a confidential, sales free, environment.

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 or visit the website www.tif.co.uk.

Delegate Organisations

18 delegates attended from 17 organisations encompassing the following industrial sectors: Financial Services, Leisure, Local Government, Manufacturing, Retail, Support Services and Utilities.

Workshop Process

The Payment Card Industry (PCI) Data Security Standard is a world-wide benchmark mandated by card schemes for the protection of cardholder identity and transaction information. From 30th June 2005, all organisations processing credit card transactions had to conform to this new Standard, but visibility of the deadline had been poor and it was imperative that the Business implications were fully considered.

At a previous tif. Information Security Service event (Retail Security 23/11/2005) issues around scope, applicability and interpretation arising from 'compliance journeys' towards the new Standard were addressed. Together with input from an online subscriber Q&A, these contributed to the agenda for this workshop, which included presentations from PCI members, a Qualified Security Assessor (QSA) and a representative of the corporate user community.

The workshop objectives were to clarify the Standard and its impact on Businesses, to take issues arising directly to representatives of the PCI for redress, and to enable professionals involved in ensuring conformity with this Standard to share best practice and experiences.

Agenda Topics

- Clarification & Scope of the PCI Standard (Presentation by PCI Representatives)
- Conflict & Relationship with Other Standards (APACS, ISO17799 etc.)
- Self Assessment Questionnaire - Data Collection, Completion, Cost, Scans & Security Site Review
- Impact on the Business

Summary

- MasterCard and Visa did not consult Merchants in creating the standard. This has led to issues being uncovered by Merchants as attempts to implement it progress
- This meeting with tif. subscribers was stated as being 'exceptional' by MasterCard & Visa since they do not engage directly with Merchants
- Payment Card compromises are growing at an alarming rate. The PCI standard must be complied with. It is a worldwide industry standard aimed at preventing payment card compromises. However, it is being perceived by Merchants as a heavy ongoing overhead
- There are Levels for Merchants based on transaction volume, and each has its own compliance requirements (i.e. actions that the Merchant must take)
- Both scans and audits are required by the PCI standard
- Acquirers are the direct interface to the Merchant and not MasterCard / Visa. Communication with Acquirers is a continual problem
- The current situation with regard to organisations being able to implement the PCI standard remains unsatisfactory

Key Issues Raised

- Transaction numbers for Merchant Levels are inconsistent
- Deadlines are set without due regard to the available lead time for adequate action
- Lack of direct information to Merchants from MasterCard and Visa. Information is propagated through Acquirers, but Acquirers and Qualified Security Assessors (QSA)s cannot answer questions of clarification about the standard
- Third party vendors must comply for some Merchants to comply. Yet Visa and MasterCard do not, in all cases, know who they are. Nor do the Acquirers
- There is conflict between the PCI standard and other standards at a detailed level. It is not clear which has primacy
- Acquirers do not inform the IT arm of the business of the existence of the standard nor tell the business that there are IT implications. In one organisation the questionnaire had been completed by the 'media people', who did not keep a copy

- It is not clear in what context to answer the questionnaire: by business, for each system, for all systems, or network
- The questionnaire is not user friendly and does not fit with other Best Practices such as COBIT and BS7799. There is no measure of risk, impact, or probability, and the limitation of Yes/No responses does not make realistic sense from a business perspective.
- Many have significant problems in completing the online questionnaire e.g. Answering Not Applicable means that a Merchant is non compliant. This is currently being addressed
- The Acquirer should not dictate which QSA is to be used.
- There is a lack of consistency of approach between QSAs e.g. there are no standard mitigating controls. Each QSA decides for itself
- QSAs are inconsistent over charging for scanning: per IP address or for all IP addresses
- There is inconsistency across QSAs over which IP addresses need to be scanned. MasterCard and Visa have no standard for this
- IP Addresses believed to be properly segregated may in fact not be. Not scanning them could lead to undiscovered vulnerabilities
- Scanning results (vulnerabilities) differ across successive scans
- There is no documented appeals process, and it can vary by QSA
- QSAs receive regular training by MasterCard and Visa, yet APACS compliance was not raised by them
- MasterCard does not read the Report on Compliance (ROC). Visa does. There is a lack of consistency which could affect acceptance of mitigating controls
- MasterCard has defined a 'fine' structure: Visa has not
- The PCI DSS (Data Security Standard): focuses on what can and cannot be stored - Full Track 2 magnetic stripe information can't be stored. Some companies currently do this and it is a major industry issue.

Summary of Agreed Actions

Corporate Users to revisit topic in 6 months time i.e. after the June '06 deadline has passed to share and resolve outstanding issues

PCI Representatives:

- to discuss the Level1 and Level2 transaction levels to ensure they are consistent
- to consult with USA colleagues regarding IVR question (speech recognition and voice recording), and communication of vulnerability level changes, reporting back to The Corporate IT Forum
- to communicate the QSA appeal process and the correct approach and processes regarding external IP Addresses (including multiple servers using one merchant number)
- to confirm which IP addresses need to be scanned, and which are covered by the PCI standard
- to communicate to delegates the set-up of the joint web site (planned live date by end of Q1)
- to have approached third party providers (aided by delegates) to ensure compliance to standards (PABP). Website to carry details
- to communicate to Acquirers the need to ensure that their contacts within the delegate organisations pass on the necessary information regarding PCI Security Standards to their respective IT departments
- to look at having one industry website for PCI

Contents of the Full Report

The following is a list of the additional material contained in the full output report from The Implications of PCI Standard Compliance 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.

- | | |
|---|----------------------------------|
| 1. Summary and Best Practice Conclusions | 4.1. Delegate Input & Q&A |
| 1.1. Key Issues Raised During Presentations | 5. Presentation: User Case Study |
| 1.2. Key Issues From Workshop Discussion | 5.1. Delegate Input & Q&A |
| 2. Presentation: MasterCard | 6. Completing the Questionnaire |
| 2.1. Overall Summary | 6.1. Issues |
| 2.2. About The PCI Standard | 7. On-site reviews |
| 2.3. The Compliance Process | 8. Merchant Levels |
| 2.4. The PCI Data Security Standard | 9. Scanning & Testing |
| 2.5. Delegate Input & Q&A | 10. Qualified Security Assessors |
| 3. Presentation: Visa | 11. AOB |
| 3.1. Delegate Input & Q&A | 12. Related Links |
| 4. Presentation: Ambiron TrustWave Ltd | 13. Actions |

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.