

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

Delegate Organisations

Four delegates attended from three large retail organisations.

Agenda Topics

- PCI Update
- Wireless networks, mobility solutions and RFID
- Management of peripheral devices
- Policy: structure, awareness and enforcement
- Security function structure
- Risk analysis

Workshop Process

Further to the success of the initial retail meeting in November 2005, a second meeting focused on mobile and wireless solutions, including a discussion regarding policies, their development and delivery. There was also an update regarding the progress with Visa and MasterCard on PCI.

Summary

- Current Compliance Timelines
 - Visa: October 2006
 - MasterCard: March 2007
 - Original Rest of the World compliance is June 2006.
 - Issue: why are the compliance deadlines different?
- Visa will fine companies in the summer of 2006 for non action, MC will fine in spring 2007
- According to MasterCard Visa only about 21% of organisations are doing a Gap Analysis
- The standard appears to still be evolving and some clarification is still required. However, delegate organisations are moving forward

- The APACS 70 issue has been resolved (end Jan)
- Its implementation *will* be a significant cost to organisations: these could be £5m-£10m, estimating cost is a major problem
- Issue: PCI is seen as an IT issue not a business one
- Have a Board/FD dialog. Set up a steering group of key stakeholders
- Common key steps appear to be
 - Do a pre-Gap Analysis data study
 - Have a Gap Analysis done by an auditor or QSA (Qualified Security Assessor)
 - Do a mitigating controls assessment
- Using the same QSA throughout the process may achieve consistency
- Most organisations would not let the people who do the Gap Analysis do the other PCI work
- There is still no definitive common understanding by delegates of what comes within scope for scanning
- Be Aware: PCI also covers paper based information
- Be Aware: opening up ports for non-PCI related tasks can breach PCI standards
- Expect the PCI standards to change as the future risks change

Subscriber comments:

"The card companies didn't talk to merchants when setting up the standards: this is like creating laws without talking to lawyers."

"PCI is on the tail of Chip and Pin, which did have a reasonable timeframe not like PCI. PCI could cost us between five and ten million pounds."

Contents of the Full Report

The following is a list of the additional material contained in the full output report from this Retail Security 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 & Best Practice
- PCI Update
- Wireless Networks, Mobility Solutions & RFID
- Management of Peripheral Devices
- Policy: Structure, Awareness, Enforcement
- Security Function Structure
- Risk Analysis
- Related Links
- 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.