

Abstract – PCI DSS Encryption & Controls #2 (WebEx)

tif. Subscriber Workshop: Tuesday 24th April 2007

THE CORPORATE IT FORUM

The Corporate IT Forum (tif.) provides an environment for IT professionals to exchange their experience of IT issues. The Forum is run by a professional management team on behalf of its corporate subscribers. These subscribers require a truly unique service: a confidential, SUPPLIER-FREE environment, in which corporate-level IT professionals openly and honestly hold discussions, attend workshops & seminars and make use of a moderated, E-mail-based Q+A service to exchange ACTUAL experiences of IT. This exchange of expertise significantly benefits both the subscribing organisations and participating individuals alike.

The Forum is extremely effective because over 3,600 corporate IT professionals, within 150+ subscribing organisations (including over half of the eligible FTSE 100), contribute over 60,000 man years' know-how and experience in implementing IT solutions. No larger knowledgebase of real-world, current IT expertise exists within the UK. The use of tif.'s expertise within its subscriber community has directly contributed to reducing IT project costs and shortening implementation timescales.

To further discuss the many benefits to your organisation of taking out a subscription to The Corporate IT Forum, contact us on 01442 866 634 or visit our website, www.tif.co.uk.

Delegate Information

7 delegates from the retail sector attended

Introduction: Workshop Scope

This is the second of two Webex events held on the same day covering PCI DSS Encryption and Controls attended by 9 organisations drawn from a variety of sectors. It raises important issues concerning compliance with the standard particularly for those who are at lower Merchant levels.

Summary

- ◇ Being ISO27001 certified or compliant will mean you have less work to do to comply with PCI
- ◇ Beware: Some audit trails contain Credit Card information e.g. PAN. Also, some audit trails are 'signed' and must not be amended for legal reasons
- ◇ Introduce card swipe machines at the Point-of-Sale that encrypt the card data. It can then be stored in its encrypted form on the back end system
- ◇ Compensating controls will only be valid for a one-year period. Source: Ambiron Trust Wave (11 May 2007):
- ◇ Some delegates are doing a 'watching brief'—the PCI standard and published timescales do not allow this approach
- ◇ There are no answers yet on how to handle data in legacy systems e.g. how to encrypt the data
- ◇ Some delegate organisations are looking at network segmentation
- ◇ Take account of (compensating) controls during system design, and restrict access by MAC/IP address if appropriate
- ◇ Reduce the number of areas where card data is stored
- ◇ Be Aware: Many systems have logging capabilities, and store card data
- ◇ Business buy In:
 - Use a risk based approach (ISO27001/BS7799) to sell projects such as this to the business
 - Use damage to Reputation as a driver.

Confidential: Corporate IT Forum

Contents of the full Report

- ◇ Summary and Best Practice Conclusions
- ◇ Deploying Encryption
- ◇ Compensating Controls: Decision Making Process & Criteria
- ◇ Getting Business Buy In to Cost
- ◇ Related Links
- ◇ Delegate Information

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.