

Abstract – PCI DSS Encryption & Controls #1 (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

4 delegates from the retail sector attended

Introduction: Workshop Scope

This is the first of two Webex events held on the same day covering PCI DSS Encryption and Controls attended by 7 organisations drawn from a variety of sectors

Summary

Strategy

- ◇ Limit the scope of PCI by reducing the number of places the full card number is held
- ◇ Confine payment and reconciliation related processes to a single application which can then be fire walled e.g. use Trintech PayWare
- ◇ If you don't keep credit card numbers then you remove the need for encryption
- ◇ Once you have authorisation then lose all knowledge of the card data
- ◇ Key Technique: remove data, storage, systems *from the scope* of the PCI standard in order to avoid the need for encryption
- ◇ Have encryption from the Point of Sale to the back end server.

Tactics

- ◇ Key Management is critical but Key Management technologies are immature, emerging, and come from very specialised suppliers/vendors
- ◇ Many systems log data, including credit card information
- ◇ Legacy Systems: Remove systems from scope by completely removing the card data, or meet the PCI standard by updating the card number to no longer be the full card number
- ◇ The PayWare vendor says it will develop a PCI compliant version of the product: this will remove a lot of the application compliance work
- ◇ SAP say the next version of SAP is planned to be PCI compliant (However for some organisations this may take some time to implement)

Confidential: Corporate IT Forum

- ◇ The PCI standard is e-commerce focused and ignores the issues it creates for Retailers with a physical presence, who face major changes to systems, and major investments, in order to meet the PCI standard

Contents of the full Report

- ◇ Summary and Best Practice Conclusions
- ◇ Deploying Encryption
- ◇ Compensating Controls: Decision Making Process & Criteria
- ◇ General Discussion
- ◇ 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.