

Abstract – Achieving PCI Compliance

tif. Subscriber Workshop: Tuesday 29th January 2008

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

20 delegates from the retail sector attended

Introduction: Workshop scope

Achieving PCI compliance is a slow and expensive process for many. This event was attended by Security and Compliance managers from 13 subscriber organisations and outlines some of the issues and solutions found on the road to becoming compliant.

Summary and Best Practice Conclusions

- ◇ IMPORTANT: ALL PCI requirements must be adhered to regardless of what merchant level you are at
- ◇ Being 85% compliant is not good enough: outstanding actions cannot be carried forward for ongoing rectification
- ◇ Current major problem areas are: encryption, network segregation, third parties, and event monitoring
- ◇ All deadline dates are already passed.

Strategy

- ◇ Reduce the scope by not holding data, and piggy back on existing mature security processes (e.g. ISO27001): this makes compliance easier to achieve and controls additional cost
- ◇ The Best Resolution is: If it is not there it does not need to be protected
- ◇ The Guiding Principles are:
 - If you don't need it then don't store it
 - If you need it: protect it/encrypt it or both—lock it up, jumble it up, keep it in as few places as possible.
- ◇ "70% of failures on PCI Level 1 compliance on first audits are due to lack of policy."
- ◇ A thorough Gap Analysis reduces the number of surprises later
- ◇ Having a flat network will bring everything within PCI scope
- ◇ Avoid the need for encryption
- ◇ Voice recording is still data, and comes within scope
- ◇ The PCI standard says that you have to log every access to card data
- ◇ Important: Do not use production data for application development testing

Confidential: Corporate IT Forum

- ◇ Have an Incident Response Plan.

Other

- ◇ Operating system trace files, and debug files are within scope
- ◇ Network Segregation is a significant task
- ◇ If vendor software is noncompliant the merchant is still responsible
- ◇ Keep a list of the status of each control
- ◇ The Merchant can select when the first audit is done.

Contents of the full Report

- ◇ Summary and Best Practice Conclusions
- ◇ Presentation PCI DSS Compliance
- ◇ Compliance
- ◇ Deadlines & Penalties
- ◇ Audit
- ◇ New Requirements in the Pipeline
- ◇ Other
- ◇ Delegate Status
- ◇ What Will You Take Away?
- ◇ 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.