

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.

Participating Organisations

Security, risk and ecommerce specialists from 9 organisations took part in this online Question & Answer discussion. Participating organisations encompassed the following industrial sectors: Energy, Local Government, Paper & Printing, Retail, Transport and Wholesale. The discussion ran between 3rd October and 13th December 2005.

QA1600 - Payment Card Industry Security Standards

A tif. subscriber requested answers to the following:

1. Have you been approached by your Acquirer regarding compliancy & been informed of compliancy deadlines?
2. Did you consider the Self-Assessment Questionnaire to be clear and unambiguous?
3. Have your websites been scanned by an accredited security company and were you satisfied with the consistency of results, in particular the vulnerabilities and their severity levels?
4. Were the scan output reports understandable and meaningful?
5. Would other organisations be interested in attending a PCIS-related event to be run by The Corporate IT Forum?

Question Background

During the previous 12 months, organisations had been required to submit their Information Security systems for scrutiny under the MasterCard/Visa Payment Card Industry Security Standards (PCIS). Initially the standards related to ecommerce sites, requiring Merchants to complete self-assessment questionnaires and submit their websites to external scans by an accredited security company. The standards were then broadened to include all elements of a business which embrace financial transactions involving payment cards.

A set of procedures and audit standards were produced to support the compliancy requirements and introduced in June 2005. Any organisation - not only retailers and financial institutions, but public sector organisations taking payments on-line for council tax, parking fines etc - now faced the prospect of having considerable fines imposed upon them for non-compliance.

The interpretation of these standards seemed to be quite open.

Question Objective

An understanding of organisations' issues with the Payment Card Industry Security Standards, as assessment of the level of interest in a tISS workshop on PCIS, and input to an agenda for such a workshop.

Summary of Responses

1. Subscribers had been misinformed about deadline dates; or not yet received a firm date for compliance; or only been informed by their acquirer after the date had passed; or were still waiting to hear from their acquirers.
2. Subscribers had found the questionnaire to be clear in some parts but unclear in others, biased towards financial institutions, and open to interpretation. They had also found a degree of ambiguity in the Standard itself.
3. Some subscribers had considered the scanning carried out by PCIS-accredited companies to be professional and were satisfied with the 'thorough' results. Others believed the tests conducted to be only superficial, rudimentary, not carried out specifically against the standard or not carried out to the same level as scans conducted by other organisations not currently PCIS-accredited.
4. In general subscribers were not overly impressed by the quality and value of the reports submitted by the accredited scanning organisations.
5. Subscribers felt a workshop would be beneficial, and most QA participants registered their interest in attending.

Actions arising from QA1600 - Payment Card Industry Security Standards

The issues raised in the online Question & Answer discussion lead to a programme of activities where subscribers discussed experiences confidentially, in subscriber-only discussions, and took their concerns and discussion output directly to key PCI representatives and their acquirers.

Contents of the Full Q&A Discussion

Subscribers to The Corporate IT Forum can download the full transcript of this, together with any other of the c2000 online Question & Answer (QA) discussions via the tif. website.

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.