

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

10 delegates attended from 7 organisations across the large-scale retail sector.

Agenda Topics

- Payment Card Industry (PCI) Standards
- How security is managed in retail organisations, including the structure and hierarchy
 - CISO/CSO - should they be a Board member?
- Understanding the typical retail security infrastructure; front-end network and node security
 - network architecture & security
 - end-device access control
 - end-device vulnerability management
 - threats to the front-end
- Identity & Access Management
 - systems in use
 - processes in place
 - dealing with high staff turnover
 - Mobile devices – securing shop-floor devices with access to back-end systems

Workshop Scope & Process

Whether national or international, retail companies face the challenge of increasing efficiency and effectiveness while at the same time protecting their brand against the competition, driving revenue and continually improving customer service as a means of building loyalty. Security has huge implications on the way this is achieved and new challenges are coming in the form of increasing regulation and legislation mandating levels of security as part of overall corporate governance. From 30th June 2005 organisations handling financial transactions online had to conform to the new PCI Security Standard, but visibility of this deadline has been poor and it is imperative that the Business implications regarding these new standards are fully considered.

The discussion was restricted to organisational representatives participating in the tif. Information Security Service (tISS), and the agenda was developed through input and responses to a tISS QA.

Summary

- In retail terms, PCI Standard will apply to e-commerce, branches, in-store concessions, third party suppliers, paper records—all data dealing with credit cards (including card indexes held by shop floor

- concessions). There is a 72 page document available, detailing the Standard, but also available is a an 'auditor's list of questions', which is more helpful in gaining an understanding of requirements
- The PCIS raises a number of significant issues: very high cost (delegates believed it might cost as much as Chip and Pin, and end to end encryption will be costly to implement); short timescale; practicability; scope; stability - the standards keep changing; lack of consultation; and lack of clarity
 - The communication and management of the standards are not being handled well by the standards' owners (MasterCard/Visa) - *"At April 2005 our main acquirer and finance division were not aware that the standards existed."*
 - The Retail Consortium is not taking any active role, is not trying to influence, and doesn't appear to know what the standards are.
 - Security organisation & structure: Commonly
 - There is a full-time security team
 - Responsibility for security implementation is usually devolved to other teams
 - The Security Manager is an organisational role.
 - Retail Security Infrastructure Front-End Network & Nodes: there are four key areas: network, end-device access control, end-device vulnerability, and threats to the front end
 - Typically retailers have two distinct networks: branch network, and HO Network
 - MAC address is a key method of control
 - Common patching approach
 - Not all Microsoft patches are applied
 - Hold regular meetings to decide which to apply based on risk
 - Use deployment tools.
 - Identity & Access Management: there are three important areas to consider: systems in use, processes in place, and staff turnover
 - Security Issue: High staff turnover in India for roles such as Unix SysAdmin and Directory Admin. Especially since service account passwords tend not to be retired frequently
 - Smart phones have Internet access but do not have content screening.

Delegate Quotes

'Good to talk to other retailers in a small group'

'It is a good 'checksum''

'Dealing with retailers with like-minded issues'

Contents of the Full Report

The following is a list of the additional material contained in the full output report from the tISS Retail Security Workshop. Subscriber-nominated tISS representatives can download any of the tISS workshop output reports, policy documents and security briefing notes available via the website.

- Summary & Good Practice
- Payment Card Industry Standards: What they are; Issues; Pushback Action Required by Retailers
- Security Structure & Hierarchy in Retail Organisations; Organisational Examples
- Retail Security Infrastructure: Front-End Network & Nodes; Network Examples; End Device Vulnerabilities (inc patching)
- Identity & Access Management; Provision of Individual Access; User Accounts; High Staff Turnover
- Mobile Devices; WiFi Detection Management & Rogue Devices
- Miscellaneous Items, Related Links & Actions
- Delegate List

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.