PCI DSS Ver. 3.0
Noteworthy Changes for Petro Retailer

A Data Security Committee Work Product

Jointly developed by
Paul Dalberth – The Pantry
Phil Schwartz – Valero
Jim Shepard – Phillips 66
Nancy Tosto – BP

5-Mar-2014

CONEXXUS
solve forward

Copyright Statement

Disclaimers

Conexxus makes no warranty, express or implied, about, nor do they assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials. Although Conexxus uses reasonable best efforts to ensure this work product is free of any third party intellectual property rights (IPR) encumbrances, it cannot guarantee that such IPR does not exist now or in the future.

Agenda

- Overview of Changes
  - Key dates
  - Areas of focus
- Table of noteworthy changes
  - Please share your best practice
- Q/A and Wrap Up

CONEXXUS
solve forward

Overview of Changes

- PCI DSS version 3.0
  - The PCI DSS digital dozen stays the same
    - The 12 core security principles don't change
  - Key dates
    - Effective 1-Jan-2014
    - Mandatory 1-Jan-2015, some requirements 1-Jul-2015
    - Probably don't want to start a version2.0 assessment in the 4th quarter of 2014.
  - More than 100 additional controls
    - More evidentiary items required to prove compliance

CONEXXUS
solve forward

Areas of Focus by SSC

- Increase rigor to protect point of sale systems
- More prescriptive requirements for
  - Vulnerability assessments
  - Penetration testing
- Third party vendor scrutiny (trust but verify)
- Inventory all in-scope components
  - Hardware
  - Software
- Scoping and segmentation

CONEXXUS
solve forward

Noteworthy Changes

- Business As Usual (BAU)
  - PCI should be part of ongoing operations every day, not just once a year when the annual assessment is done
  - Bob Russo: “make PCI your compass not your map”
  - Impact: Low
- Implementation Guidance
  - Security must be 24/7 x 365 days
  - Keep abreast of PCI changes
  - Monitoring is critical
    - Vulnerability announcements
    - Remote access
    - System logs
    - Etc., etc.

CONEXXUS
solve forward

Noteworthy Changes

- Requirement: 2.4
  - Maintain an inventory of system components that are in scope for PCI DSS
  - Estimated Impact: **High**
- Implementation Guidance
  - Verify that a list of hardware and software components is maintained and includes description of function/use for each. Include point of sale system, CRINDs, and other point of interaction (POI) devices
  - Have a process to ensure inventory is kept current
  - Will help to accurately and efficiently define scope of environment for implementing PCI DSS controls. Without an inventory, some system components could be forgotten.

CONEXXUS
solve forward

Noteworthy Changes

- Requirement: 9.9
  - Protect devices that capture payment card data from tampering and substitution
  - Estimated Impact: **High** Effective 1-Jul-2015
- Implementation Guidance
  - Maintain list of all devices (Requirement 2.4)
  - Periodically inspect devices for tampering or substitution
  - Take pictures of the devices and use these during inspection to see whether it has changed.
  - Mark devices with a special label or secure marker pen, such as a UV light marker.
  - Train personnel to detect evidence of tampering or substitution of POI devices.

CONEXXUS
solve forward

Noteworthy Changes

- Requirement: 11.3.3
  - New requirement to develop and implement a methodology for penetration testing
  - New requirement to correct exploitable vulnerabilities found during penetration testing and repeat testing to verify corrections.
  - Estimated Impact: **High,** Effective 1-Jul-2015
- Implementation Guidance
  - Penetration testing methodology must adhere to an industry standard, such as NIST SP 800-115.
  - Perform penetration testing when moving to a new OS level (i.e., Windows XP to Windows 7).

CONEXXUS
solve forward

Noteworthy Changes

- Requirement: 11.3.4
  - If segmentation is used to isolate the CDE from other networks, perform penetration tests to verify that the segmentation methods are operational and effective.
  - Estimated Impact: **High,** Effective 1-Jul-2015
- Implementation Guidance
  - Penetration testing is an important tool to confirm that any segmentation in place to isolate the CDE from other networks is effective.
  - If the border isn't there (i.e., your segmentation isolating the CDE), then the scope of your assessment just grew, substantially. Possibly to the entire enterprise.

CONEXXUS
solve forward

Noteworthy Changes

- Requirement: 12.8.5
  - Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
  - Estimated Impact: **High,** Effective 1-Jul-2015
- Implementation Guidance
  - Document which PCI DSS requirements are managed by your service providers.
  - If the service provider offers a variety of services, this requirement should apply to those services delivered to you (the client), and those services in scope for your PCI DSS assessment.
  - The intent is to improve management of third party service providers and provide greater visibility into managed cloud services.

CONEXXUS
solve forward

Noteworthy Changes

- Requirement: 5.1.2
  - Evaluate evolving malware threats for any systems not considered to be commonly affected by malicious software.
  - Estimated Impact: Medium
- Implementation Guidance
  - Industry trends for malicious software can change quickly, so it is important for organizations to be aware of new malware that might affect their systems
  - Monitor vendor security notices and anti-virus news groups to determine whether their systems might be coming under threat from new and evolving malware.

CONEXXUS
solve forward

Noteworthy Changes

- Requirement: 1.1.2 and 1.1.3
  - Clarified what the network diagram must include and added new requirement at 1.1.3 for a current diagram that shows cardholder data flows within the cardholder date environment (CDE).
  - Impact: Medium
- Implementation Guidance
  - Cardholder data-flow diagrams identify the location of all cardholder data that is stored, processed, or transmitted within the network.
  - Have a formalized process to define what/where the CDE resides – where it is and where it is not
  - Keep diagrams current, document your updates

CONEXXUS
solve forward

Noteworthy Changes

- Requirement: 8.1.5
  - Clarified the requirement for remote vendor access applies to vendors who access, support or maintain system components, and that it should be disabled when not in use.
  - Estimated Impact: Low, Effective 1-Jul-2015
- Implementation Guidance
  - Service providers must have different authentication credentials for their customer's environment. This could be significant for systems integrators
  - Enable remote access only for the time period needed, then disable
  - Monitoring vendor access provides assurance that vendors are accessing only the systems necessary and only during approved times.

CONEXXUS
solve forward

Noteworthy Changes

- Requirement: 2.1
  - Changing vendor default passwords applies to all default passwords, including systems, applications, security software, terminals, etc. and that unnecessary default accounts are removed or disabled.
  - Estimated Impact: Low
- Implementation Guidance
  - Change default passwords, please! Numerous data breaches due to default passwords not being changed at implementation time
  - Include default accounts that won't be used. Changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

CONEXXUS
solve forward