PCI DSS 3.0, The Good, The Bad The Confusing

ISSA Denver, 12 December 2013

Intros/Agenda

- Who is this guy?
  - History with PCI DSS
  - PCI Compliance, 3e
  - Blog
  - BoA 2011-2013
- How can I help?
  - Q/A
  - Consulting
- Want to stalk me?
  - @BrandenWilliams
  - U CAN HAZ SLIDEZ

History of PCI DSS 3.0

- Key Dates for 2013:
  - Release date: November 7, 2013
  - Draft published to POs on September 12
  - Most of the changes published there are intact
- Lifecycle Notes
  - 2010 changed from 2 years to 3
  - No errata published in 2.0
  - Review/Feedback lead to 3.0
- Effective date, 1/1/2014
- PCI DSS 2.0 retire date: 12/31/2014

Documents for Use

- Today:
  - PCI DSS 3.0
    - Includes Navigating PCI DSS
    - Plus updated Reqs
  - PA DSS 3.0
  - Diff documents
- Soon:
  - SAQs
  - Glossary?
  - Prioritized Approach?
- www.pcisecuritystandards.org

Themes that drove PCI DSS v3.0 changes

- Education and Awareness
- Increased Flexibility
- Security as a Shared Responsibility
- Fix the following:
  - Lack of education and awareness
  - Weak passwords and authentication practices
  - Third party risks
  - Limited capability to detect breaches and/or malware
  - Lack of consistency in assessment

Executive Summary Changes

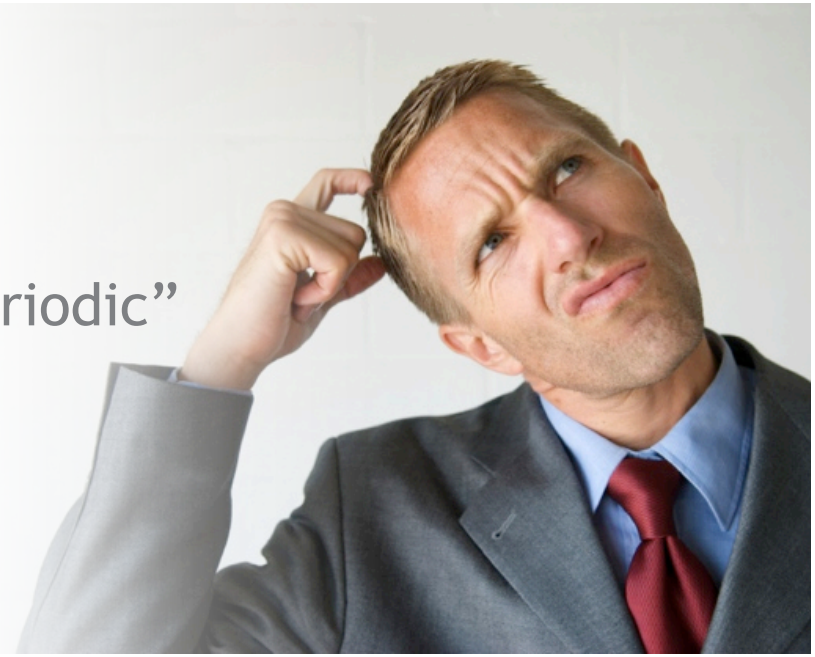
- Executive Summary:
  - Scoping Clarifications (examples & added guidance)
  - Business as Usual Section
    - What the… ?
    - Agree something could be done
    - Cart before horse
    - NO REQUIREMENTS!
  - Scoping separate from Sampling
- ROC Reporting Instructions
  - Now separate document

Some Words on Scoping

- Responsibility for scoping is that of the organisation under assessment
- A QSA does not define the scope of an assessment
- A QSA validates the scope that has been determined by the organisation as part of the assessment

Now, here's something strange…

- Biggest complaint about PCI DSS process:
  - Too Restrictive (let me do risk mgt)
  - Too Loose (tell me what I have to do)
  - Too much interpretation variance
- Two sides to every room:
  - TOO RESTRICTIVE
  - TOO OPEN FOR INTERPRETATION
- Council waged war: "should" & "periodic"
- New version reverses trend:
  - Periodic: 20 times (up from 8)
  - Should: 103 times (up from 27)



Some of the Great Additions

- From the “How do you do this without these instructions” dept
  - Cardholder Data Flow diagrams required
    - Don’t do this on a network diagram
    - See “Data Flows Made Easy”
  - Managing list of in-scope systems
    - Helps with scoping overall
    - Cloud/Virtualization.. Whaaaa?
    - Could be a challenge

- Overall, the documentation requirements are much higher
- Be sure to allocate time and resources to this (automation potential!)

Some of the Ugly, Weird, or Questionable

- Malware discovery:
  - On platforms NOT commonly affected
  - Yes, you read that right
  - Interpretation will be interesting
- Penetration Testing:
  - Approved methodology
  - Approved by…
  - Why not reference SP800-115?
- Lack of Linkage to Emerging Tech
  - Where is Mobile?
  - What about NFC?

Interesting Changes By Requirement

- Policy Documentation, by requirement
  - Well Intentioned
  - Questionably Executed
  - Each of the 12 major has one at the end
  - “Gather your docs, make sure they are good.”
- Requirement 1.4:
  - Install firewalls on MOBILE devices?
  - Soooo, firewall in the app store?
  - QSA interpretation issues galore!
  - Guidance info helps (managed by corp policy)

Interesting Changes By Requirement (cont.)

- Requirement 2.2.2-2.2.3:
  - What is a necessary service?
  - Not much changed here, just a missed opportunity
- Requirement 3.2:
  - CLARITY! YAAAAY!
  - Secondary Auth Data must be rendered UNRECOVERABLE
  - Can’t really get around that one
- Requirement 5.3 (abuse?):
  - Guess what? You can’t disable AV anymore!
  - And it must be running
  - Well, sorta. Management auth, case-by-case basis

Interesting Changes By Requirement (cont.)

- Requirement 6.2:
  - Overall like the changes… BUT!
  - Recent research shows priorities should not follow CVSS
- Requirement 7.1.1:
  - Access must be documented BY ROLE
  - Needs vs. Wants
  - Still includes least-privilege
- Requirement 8:
  - Lots have changed
  - Much more flexible around auth
  - Overall, very positive (though again, interpretation issues?)

Interesting Changes By Requirement (cont.)

- Requirement 9.9*:
  - This one is going to be a biggie
  - Anti-tampering at POI
  - Absolutely needed, closes big loophole
- Requirement 10.6:
  - Specific requirements around log review
  - Overall, much improved
- Requirement 11.1.1:
  - Show of hands, how many have Wireless in CDE?
  - Now must maintain inventory w/biz justification

Interesting Changes By Requirement (cont.)

- Requirement 11.3.4:
  - Now must test segmentation
  - Verify it is working as designed
- Requirement 11.5.1:
  - Must respond to alerts generated by change-detection
  - Keep docs on how you resolve!
- Requirements 12.8.5 and 12.9:
  - Updates to maintain list of service providers
  - With what they specifically do
  - And their level of compliance
  - And their agreement in writing

Overall Impressions

- 3.0 does do good things
  - Clarifications
  - Intent language included in standard
- 3.0 also creates lots of room for interpretation
  - Should/Periodic
  - Be sure your QSA is knowledgeable
- And leaves some things behind
  - What about Mobile?
  - Zigbee?
  - Stripe to EMV to CNP via Mobile?
  - Other emerging standards?


sysnet.
global solutions.
Thank you,
Any questions?