PCI DSS the Trilogy: Adapting Compliance Strategies to Version 3.0

Pierre Tagle, Ph.D.

Practice Lead – GRC

Outline

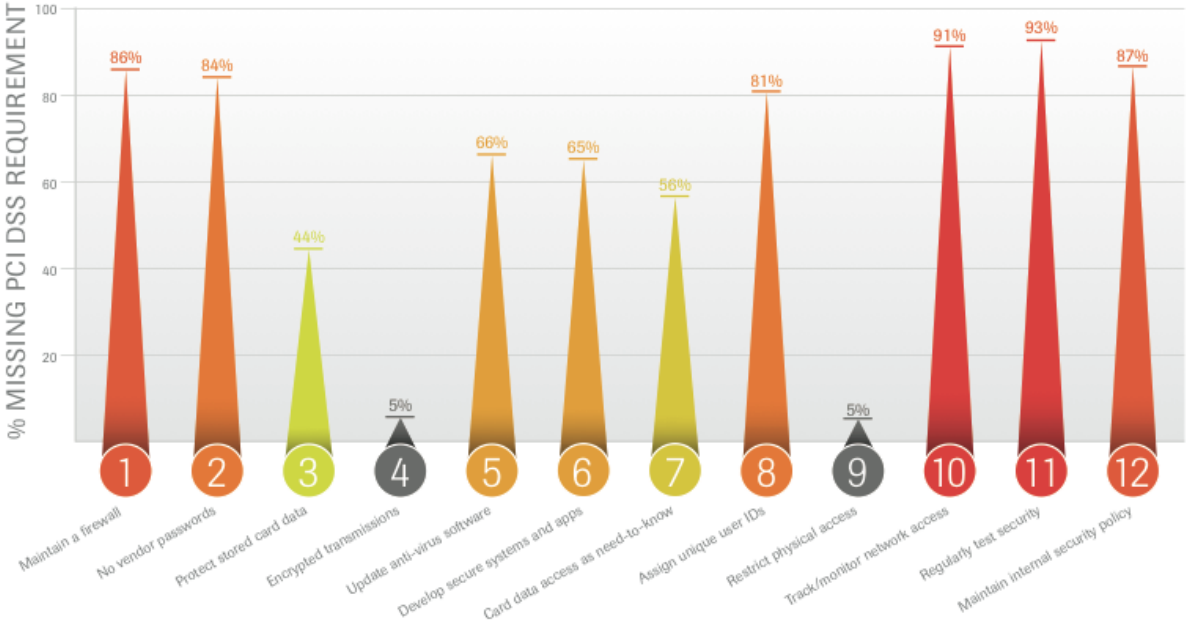
- PCI DSS v3 Timeline
- Why PCI DSS v3?
- Summary of Changes
- Reporting Compliance
- Implementation Tips

PCI DSS v3 Timeline

- 7 Nov 2013 – PCI DSS v3 is published
- 1 Jan 2014 – PCI DSS v3 comes into effect
  - Organisations can comply to PCI DSS v2 or v3
- 31 Dec 2014 – PCI DSS v2 phased out
- 1 Jan 2015 – Must comply with PCI DSS v3
- 1 July 2015 – “Best practice” requirements becomes “MUST” requirements

Why PCI DSS v3?

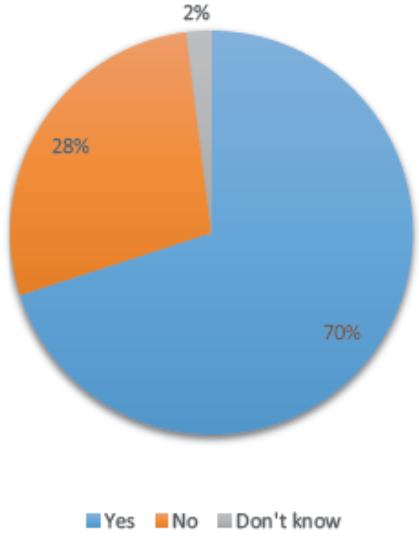
- Common PCI mistakes
- Divergent interpretations
- Slow breach detection
- Third parties



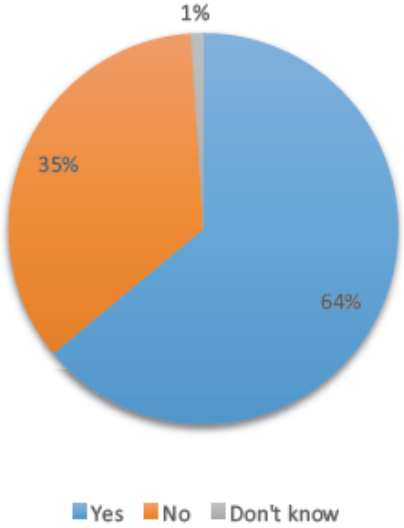
Trustwave 2012 Global Security Report

Third Parties

Do you outsource some or all of your IT infrastructure and/or support?



Do you have a lot of external interfaces to other vendors/environments?



Source: Australian Data Privacy Index April/May 2013 (Informatica)

Classifying the Changes

- **Evolving Requirement –** Changes to the standard to keep pace with emerging threats and changes in the market (i.e. these are new!)
- **Additional Guidance –** Provide more detailed information/guidance to improve understanding of the requirement.
- **Clarification –** Additional concise wording to clarify intent of requirement.

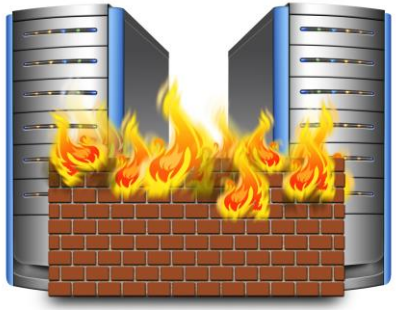
Overview of Changes in 3.0

- Scope
  - More rigor in determining what is “in scope” for assessment
- Segmentation
  - Adequacy of segmentation (tested via penetration testing)
- Third Parties
  - PCI DSS compliant in their own right, or be participant in the assessment
- Documentation
- Business as Usual
  - Monitoring of controls
  - Management/review of changes to environment, organisation
  - Periodic review of controls vs. annual audit
  - Separation of duties (operations vs security management)
  - Operational procedures
- Physical security
  - Inventory, tampering checks, training

CHANGES BY REQUIREMENT

Requirement 1

- Network diagrams must include CHD flows across systems & networks
- Clear boundaries (e.g. segmentation) → higher bar to achieve "segmentation"



Requirement 2

- Maintain inventory of all system components in scope for PCI DSS
- Business as usual function for configuration management

Requirement 3

- No significant changes

- Clarifications
  - SAD handling after authorisation
  - Logical access for disk encryption is separate from OS, and decryption not associated with user accounts
  - Key management procedures

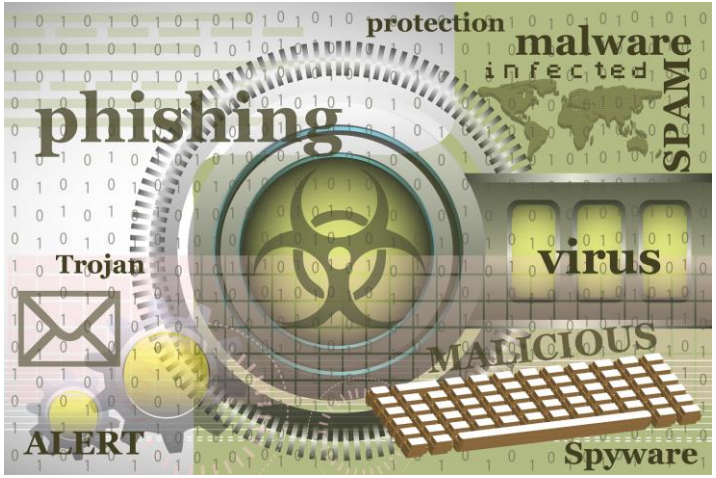
Requirement 4

- No significant changes

- Clarifications:
  - Trusted keys and certificates
  - Secure version and configuration of protocols
  - Appropriate encryption strength

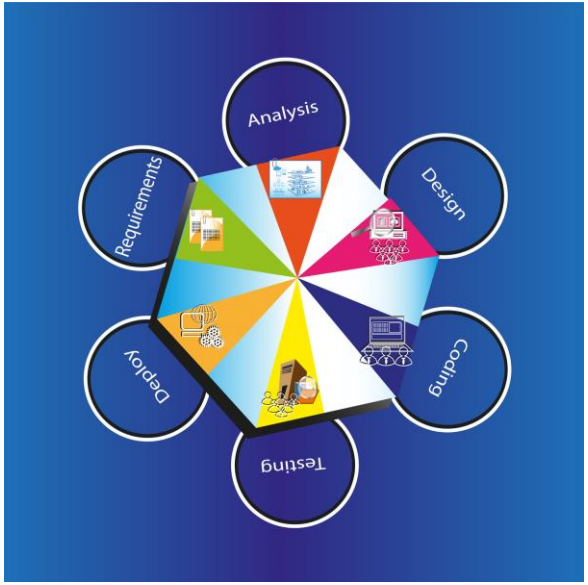
Requirement 5

- Prevent malware (not just viruses)
- Evaluate evolving malware threats for any systems not considered to be commonly affected by malicious code.
- Ensure anti-virus solutions are active and cannot be disabled or altered by users – unless specifically authorised by management on a case-by-case basis



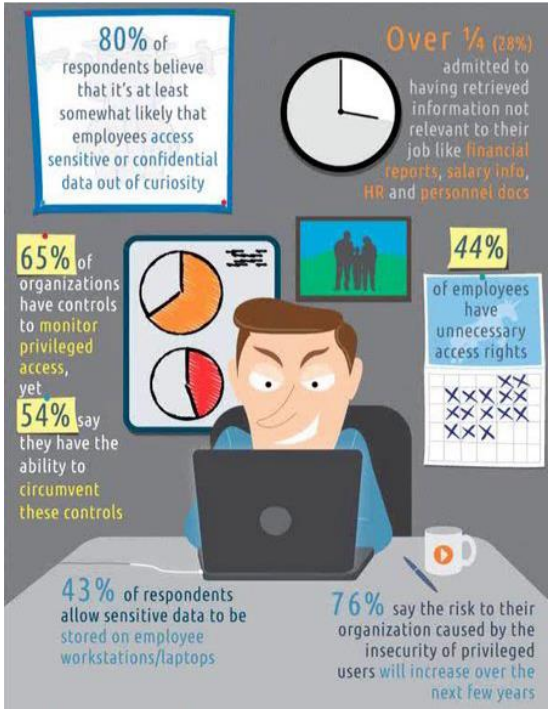
Requirement 6

- Document how PAN and SAD is handled in memory (by 1 July 2015)
- Coding practices expanded to include broken authentication and session management (by 1 July 2015)
- Clarifications:
  - written SDLC processes;
  - risk ranking & patch management;
  - Dev/Test vs Pre-Prod (plus access controls),
  - WAF = “automated technical solution that detects and prevents web-based attacks”



Requirement 7

- No significant change
- Clarifications:
  - Definitions of access needs for each role
  - Limit privileged user IDs to least privilege necessary



Source: beyondtrust.com

Requirement 8

- Flexibility to meet password complexity and strength requirements (e.g. passwords/phrases)
- Service providers with access to customer environments MUST use different credentials per customer
- Where other authentication mechanisms are used (e.g. tokens, smart cards) that the mechanisms are linked to an individual account

- Clarifications:
  - Protecting credentials (user + application/ service accounts)
  - Third party accounts
  - Remote access (disable accounts when not in use)

Password1	38.7%
password	34.5%
Welcome1	16.0%
123456	12.6%
P@ssw0rd	11.8%
Passw0rd	10.9%
Password123	10.9%
Password2	10.1%
Summer12	10.1%
password1	10.1%

Source: Trustwave Global Security Report 2013

Requirement 9

- Physical security access requirements and procedures to sensitive areas apply to onsite personnel

- Protection of physical devices (e.g. POS components) and maintenance of list / location of devices
- Training for personnel

Requirement 10

- Identification and Authentication
  - Log elevation of privileges
  - Log any changes (modification/creation/ deletion) to accounts with admin privileges
- Audit Logs
  - Capture stopping or pausing of logs (in addition to initialisation/re-start)
- Clarifications:
  - Audit trails to link access to system components to each user, and that all CHD access is included
  - Log reviews

Requirement 11

- Develop & implement penetration testing methodology – effective 1 July 2015 (e.g. NIST 800-115)
- Penetration testing MUST validate segmentation if used, i.e. compromise in non-CDE will not result in a breach of the CDE)
- Maintain inventory of wireless APs
- Compare (i.e. integrity monitoring) critical files at least weekly AND emphasis to evaluate/investigate detected changes
- Respond to alerts!

Source: chaininstitute.com

Requirement 12

- Annual risk assessment annually or after significant changes to the environment
- Third party / service provider requirements
  - Maintain scope for internal vs. third party
  - Written acknowledgements
  - Provide PCI DSS certification or be subject to the company's PCI DSS assessment
- Moved operational procedure requirements to requirement 1 to 11

REPORTING COMPLIANCE

Reporting Compliance

- Report on Compliance (ROC) vs Self-Assessment Questionnaire (SAQ)
- Rules have not changed
  - Merchant levels 1, 2, 3, 4
  - Service provider levels 1, 2

The New ROC Template

- Template driven
  - In Place
  - In Place with CCW
  - Not Applicable
  - Not Tested
  - Not in Place
- Emphasis on “less wordy” responses

PCI DSS Requirements and Testing Procedures	Reporting Instruction	ROC Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place with CCW	N/A	Not Tested	Not in Place
1.1 Establish and implement firewall and router configuration standards that include the following:							
1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:							
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.							
1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections, and • Changes to firewall and router configurations.	**Identify the document(s)** reviewed to verify procedures define the formal processes for:						
	▪ Testing and approval of all network connections.	*<Report Findings Here>*					
	▪ Testing and approval of all changes to firewall and router configurations.	*<Report Findings Here>*					
1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	▪ **Identify** the sample of records for network connections that were examined.	*<Report Findings Here>*					
	▪ **Identify** the responsible personnel interviewed who confirm that network connections were approved and tested.	*<Report Findings Here>*					
	Describe how the sampled records were examined to verify that network connections were:						
	▪ Approved	*<Report Findings Here>*					
	▪ Tested	*<Report Findings Here>*					
1.1.1.c Identify a sample of actual changes made to firewall and router configurations,	▪ **Identify** the sample of records for firewall and router configuration changes that were examined.	*<Report Findings Here>*					

Source: PCI SSC “PCI_DSS_v3_ROC_Reporting_Template.pdf”

The SAQs

- Refresh to the SAQs plus 2 new ones
- Clarifications regarding applicability
- Separate SAQ-D for Merchants and Service Providers

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP*	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP*	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

** New for PCI DSS v3.0*

Source: PCI SSC "Understading SAQs_PCI_DSS_v3.pdf"

The SAQ A-EP Apocalypse?

- Created quite a bit of debate

What types of e-commerce implementations are eligible for SAQ A-EP vs. SAQ A?

To be eligible for SAQ A, e-commerce merchants must meet all eligibility criteria detailed in SAQ A, including that there are no programs or application code that capture payment information on the merchant website. Examples of e-commerce implementations addressed by SAQ A include:

- Merchant has no access to their website, and the website is entirely hosted and managed by a compliant third-party payment processor
- Merchant website provides an inline frame (iFrame) to a PCI DSS compliant third-party processor facilitating the payment process.
- Merchant website contains a URL link redirecting users from merchant website to a PCI DSS compliant third-party processor facilitating the payment process.

If any element of a payment page delivered to consumers' browsers originates from the merchant's website, SAQ A does not apply; however, SAQ A-EP may be applicable. Examples of e-commerce implementations addressed by SAQ A-EP include:

- Merchant website creates the payment form, and the payment data is delivered directly to the payment processor (often referred to as "Direct Post").
- Merchant website loads or delivers script that runs in consumers' browsers (for example, JavaScript) and provides functionality that supports creation of the payment page and/or how the data is transmitted to the payment processor.

Source: PCI SSC "Understading SAQs_PCI_DSS_v3.pdf"

SAQ Responses

- No longer a simple Yes or No form
- Similar to ROC check list

Source: www.todaytranslations.com

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.1	Are firewall and router configuration standards established and implemented to include the following:						
1.1.1	Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	▪ Review documented process ▪ Interview personnel ▪ Examine network configurations	☐	☐	☐	☐	☐
1.1.2	(a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	▪ Review current network diagram ▪ Examine network configurations	☐	☐	☐	☐	☐
	(b) Is there a process to ensure the diagram is kept current?	▪ Interview responsible personnel	☐	☐	☐	☐	☐
1.1.3	(a) Is there a current diagram that shows all cardholder data flows across systems and networks?	▪ Review current dataflow diagram ▪ Examine network configurations.	☐	☐	☐	☐	☐
	(b) Is there a process to ensure the diagram is kept current?	▪ Interview personnel	☐	☐	☐	☐	☐
1.1.4	(a) Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	▪ Review firewall configuration standards ▪ Observe network configurations to verify that a firewall(s) is in place	☐	☐	☐	☐	☐

IMPLEMENTATION TIPS

Adapting to Version 3.0

- Review need to process, transmit and/or store CHD
- Assess gaps between v2 and v3 requirements
  - What are the technology considerations?
  - What process and/or documentation changes are needed?
  - How long to implement changes?
  - Assess necessary expertise and technology requirements
- Document migration plans

Simplifying Compliance

- When is access to CHD needed? And by whom?
- Is storage of CHD required?
- Where is access to CHD required? (branches?)
- Consider scope reduction options, e.g. segmentation, tokenisation, P2PE
- Which part of the CDE relies on third parties? Do they have access to CHD? Are they PCI DSS compliant?

Processes & Documentation

- Network diagrams and cardholder data flows
- Asset inventories – systems, networks, WAPs, devices, etc.
- Secure coding and testing
- Penetration testing methodology

Processes & Documentation

- Risk management
- 3rd party management and delineation of responsibilities
- Incident response plan
- Operational procedures across Requirements 1 to 11

Technology Areas

- Segmentation architecture/configuration (e.g. Firewalls, VLANs, IPS/IDS, etc.)
- Log management
- File integrity monitoring
- Encryption and key management
- Malware handling

Moving Forward with PCI DSS

- Compliance driven security? Or Security driven compliance?
- Integrate compliance measures into “Business-as-Usual” – on-going fluid process rather than a once a year audit concern
- Leverage or align with existing security frameworks & controls
- Periodic review of your need to handle CHD.

Thank you - Questions?

Pierre Tagle, Ph.D.

pierret@senseofsecurity.com.au

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au