

Are you really PCI DSS Compliant?



ROBERT YOUNCE
CHRISTIANA CARE HEALTH SERVICES



Agenda



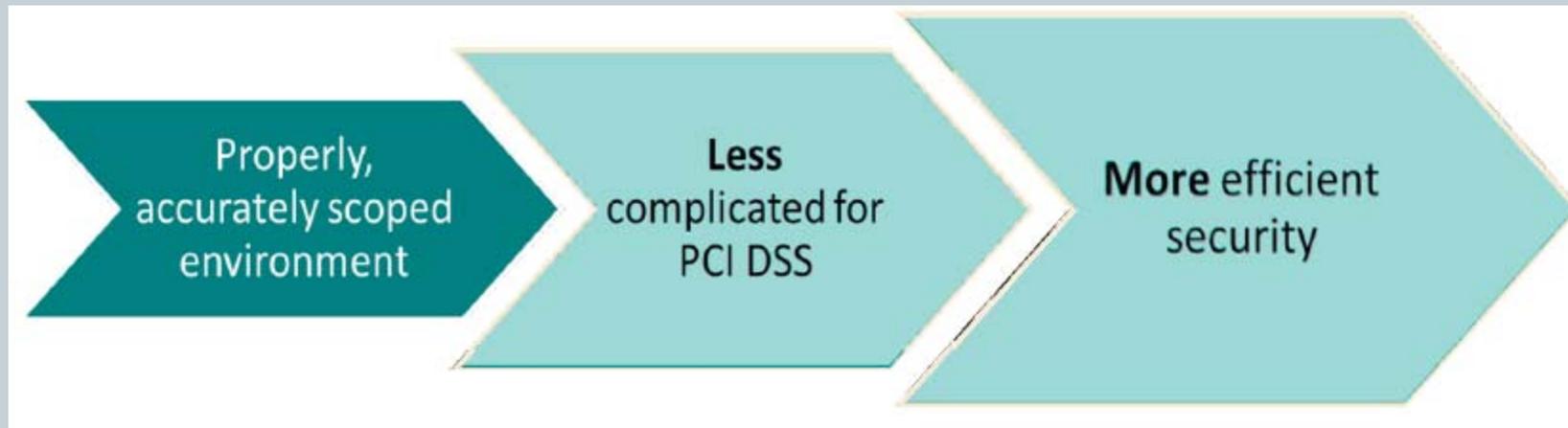
- Why PCI DSS Scoping is a Hot Topic
- PCI DSS Scoping, Misconceptions and Clarifications
- Top Tips for PCI DSS Scoping
- Wrap-up and Questions

Key Points to Remember...



- Improper scoping puts your business at risk
- Focus on security, not compliance
- Scoping is not a one-time activity
- Understanding segmentation is key

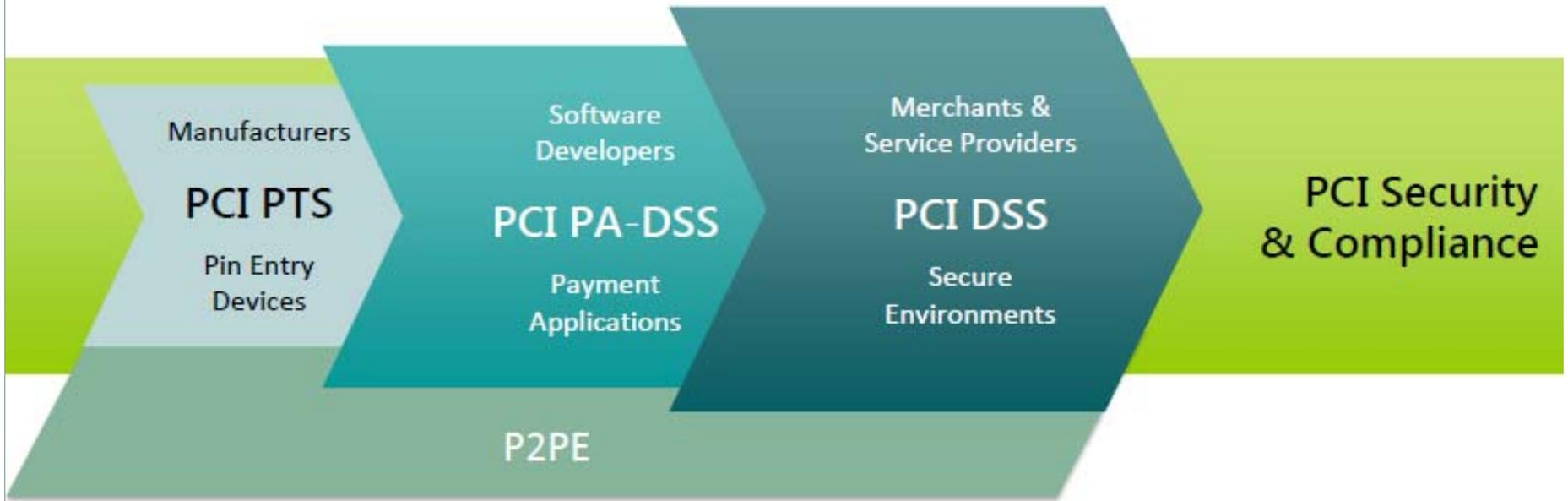
Less is More



PCI Security Standards



Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

What Does PCI DSS Say?



- PCI DSS requirements apply to all system components included in or connected to the CDE
- If network segmentation is used, the assessor must verify it is adequate to reduce PCI DSS scope
- Adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not
- Specific implementations of network segmentation are highly variable

Why PCI DSS Scoping is a Hot Topic



- **Bad interpretations and/or motivations can lead to**
 - Aggressive or accidental under-scoping
 - Ineffective segmentation controls
- **Which can have disastrous consequences**
- **Bad interpretations can also lead to unnecessary over-scoping**
 - Can result in ineffective allocation of security resources

Common Misconceptions & Misunderstandings



- I am “compliant” therefore I am secure
- My data is out of scope because <insert “silver bullet” here>
- I know where all my CHD is – it’s in my CDE
- Controlled access = segmentation = isolation?
- General scope confusion
- My vendors do my compliance for me

Compliance vs. Security



- **A “compliant” result means:**
 - Policies and processes are in place
 - Personnel are aware of the processes
 - Systems were verified to be secure
- **A compliance validation does not mean:**
 - There will never be vulnerabilities in the future
 - All personnel will follow the processes at all times
 - All systems will continue to be maintained securely
 - The environment will continue to be secure
- **Security involves maintaining compliance and includes:**
 - Understanding of environment and associated risk
 - Controls to meet PCI DSS requirements are appropriate for the level of risk
 - Checks and balances help to ensure people follow processes at all times
 - All systems are periodically verified as secure

Isn't my data out of scope because...?



Don't start with the assumption that encrypted data is out of scope, instead start from the premise that all encrypted data is in scope until proven (verified) otherwise

What is Segmentation?



- To be out of scope: segmentation = isolation = no access
- Controlled access \neq isolation
 - Controlled access:
 - ✦ Is still access
 - ✦ Is a PCI DSS requirement
 - ✦ Does not isolate one system/network from another
 - ✦ Provides entry point into CDE
 - ✦ Is in scope for PCI DSS
- If it can impact the security of the CDE, it is in scope

All my CHD is in my CDE. Isn't it?



In 66% of data breaches, the organization didn't know the data was on the system that was compromised.

Verizon 2008 Data Breach Investigations Report

Scoping Confusion?



- What does “in scope” mean?
 - Every PCI DSS requirement may not apply to an in-scope system. Consider:
 - ✦ Requirements applicable for system function/use
 - ✦ Requirements applied at network level rather than on every system
 - ✦ Controls to reduce applicability of certain PCI DSS requirements (must be verified!)
- What does “out of scope” mean?
 - Consider as ‘untrusted’
 - No security evaluation or validation of the system/network
 - If an “out-of-scope” system could lead a CDE compromise, it should not have been considered out of scope

Doesn't my vendor do my compliance for me?



- **An entity cannot outsource their PCI DSS responsibility**
 - May outsource operational responsibility for maintaining security controls
- **Vendors aren't always secure**
 - Vendors may need to be included in your PCI DSS assessment
 - Consider all relationships - vendor, integrator/reseller, IT delivery
 - Common weak points include insecure remote access and default/shared passwords

Top Tips for PCI DSS Scoping



- TIP #1: Plan your Scoping
- TIP #2: Think Outside the Box
- TIP #3: Risk Assessments as a Scoping Aid
- TIP #4: Keep your Scope Up-to-Date
- TIP #5 Trust but Verify
- TIP #6: Confirm your Segmentation
- TIP #7: Don't Rely on "Silver Bullets"

Wrap-up and Questions



Contact Info: ryounce@christianacare.org

Link: <http://www.pcisecuritystandards.org>

Remember...



- Improper scoping puts your business at risk
- Focus on security, not compliance
- Scoping is not a one-time activity
- Understanding segmentation is key