The PCI Security Standards Council
PCI DSS Virtualization Webinar

Bob Russo, General Manager
Kurt Roemer, Citrix Systems, PCI SSC Virtualization SIG Chair
June 2011
Agenda

1. Introductions
2. Council & Virtualization SIG Overview
3. PCI DSS Virtualization Guidelines
4. FAQ
5. Council Opportunities
About the Council

Open, global forum
Founded 2006

Responsible for PCI Security Standards

- Development
- Management
- Education
- Awareness
PCI Security Standards

Payment Card Industry Security Standards
Protection of Cardholder Payment Data

Ecosystem of payment devices, applications, infrastructure and users
**Objective:** Recommend changes, clarifications or improvements to the PCI Standards and the programs that support them

**Approach:** Leverage PCI SSC Participating Organizations’ valuable business and technical experiences, to collaborate with the PCI SSC on any supporting guidance or special projects relating to the PCI Security Standards

**Result:** Deliver actionable support documentation, specific instruction or recommendations to clarify how a specific technology can affect an organization’s compliance with specific PCI DSS requirements

**PCI SSC Special Interest Groups (SIG)**

- Virtualization
- Wireless
- EMV
- Encryption
Special Thanks to the Virtualization SIG!
Guidance, Not Requirements

• PCI DSS requirements still apply

• This is further clarification – does not introduce new requirements

• Not an endorsement of virtualization or any technology

• We are committed to delivering guidance on how technology can meet all stakeholder’s expectations of securing payment card data
PCI DSS Virtualization Guidelines

Different technology, same rules apply

Benefits must be commensurate with risks

No one size fits all approach

For optimal security, it’s recommended that all virtualization components meet PCI DSS requirements (out-of-scope systems can benefit from PCI security, too!)
At a Glance – Key Recommendations

- Evaluate the risks
- Virtualization leverages “virtual system components” that must meet PCI DSS requirements
- Implement ‘defense in depth’
- Isolate security functions
- Control access, even more than physical systems
- Choose your hypervisor carefully
What About Cloud Computing?

Cloud Computing

- is the use of computing as a service or utility
- can be used to deliver PCI applications and workloads
- has unique benefits, risks, and management aspects
- is rapidly evolving
Cloud Computing: What to Watch for...

• Understand how cloud will impact scoping
• Perform detailed risk assessment
• Recognize challenge of assigning responsibilities across a shared infrastructure
• Define service provider contracts
• Determine mixed-mode usage and protections
• Ensure multi-tenant isolation of PCI data
• Address added risk in public cloud environments
PCI DSS Virtualization FAQ

- As a QSA, do I need to provide all of these recommendations to merchants and processors for them to achieve PCI DSS compliance?
- What are considered the major risks that virtualization technology introduces to the payments environment?
- What is meant by mixed-mode computing and what recommendations are provided around it?
- How is virtualization different from cloud computing from a PCI perspective?
- Is it possible to be PCI compliant without following these guidelines?
- How should those in the payment chain use this guidance?
- Are all virtualized components considered in scope when it comes to PCI?
- Does the Council recommend the use of virtualization technology in this guidance?
- With current SIG projects now concluded, what is the future of Council Special Interest Groups?

Please visit our website at www.pcisecuritystandards.org
Summary

- We’re focused on developing and maintaining security requirements for the protection of cardholder data environments

- We are committed to delivering guidance on how technology can meet all stakeholder’s expectations of securing payment card data

- SIG guidance is product of industry feedback and collaboration – thank you to the Virtualization SIG and all those who’ve participated in SIG projects!

- We count on this partnership to make sure we’re giving you what you need to secure your data

- We need your continued involvement in this process
Don’t Miss These Opportunities from the SSC!

TRAINING
• ISA Training: July 11th – 12th, Toronto, Canada
• QSA Training: July 13th – 14th, Toronto, Canada
• PA-QSA Training: July 15th – July 16th, Toronto, Canada
• PCI Awareness Training Online anytime!
• Visit: https://www.pcisecuritystandards.org/training/index.php

PCI SSC 2011 COMMUNITY MEETINGS
• North America: September 19th -22nd, Scottsdale, AZ
• Europe: October 17th – 19th, London, United Kingdom
• Sponsorship opportunities are available!
• Visit: cmsponsorship@pcisecuritystandards.org.

JOIN THE CONVERSATION! @PCI SSC
• Connect with us on Twitter and LinkedIn for real-time updates on Council initiatives and upcoming opportunities for involvement.