How to Evolve Your Compliance Program As Technologies and Mandates Change

Richard E. Mackey, Jr.

Vice President, SystemExperts Corporation

dick.mackey@systemexperts.com

Agenda

- Change is constant
- Change in regulations
- Evolution of technology
- Virtualization and compliance
- Cloud computing and compliance
- Encryption requirements
- Testing

Change is Constant

- Compliance with any regulation or contract requires adaptation
  - Regulations change
  - Organizations change
  - Business risks change
  - Technologies change
  - Interpretations change
  - Auditors' processes change

Example Regulatory Changes

- PCI has changed in a number ways between 1.1 and 1.2 (October 2008)
  - Requirement for strong encryption for wireless
  - Requirement for quarterly Approved Scanning Vendor vulnerability scans – all Internet addresses
- MA identity theft law
  - Encryption of portable devices
  - Strong governance, risk assessment, policy requirements
- HIPAA
  - More audits

Technology Changes

- Virtualization
  - Combining systems while maintaining logical separation
  - Forcing auditors to make decisions
- Cloud computing
  - Outsourced flexible computing
  - More difficult decisions given less information about implementation
- Storage
  - SANs provide shared storage
- Federated security
  - Places responsibility and trust across organizations

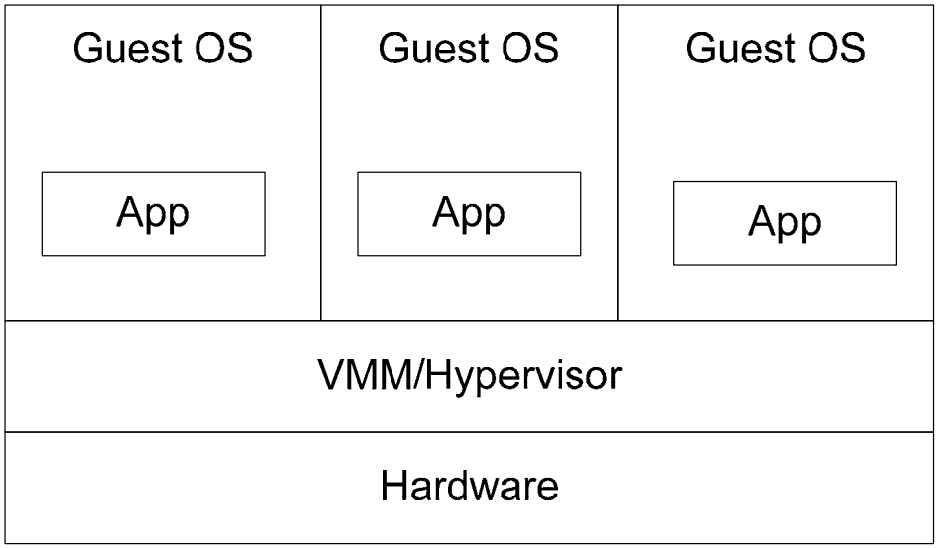
PCI CDE Scope

- *Cardholder Data Environment:* Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI DSS assessment. A cardholder data environment is comprised of system components.
- *System Components:* Any network component, server, or application included in or connected to the cardholder data environment.

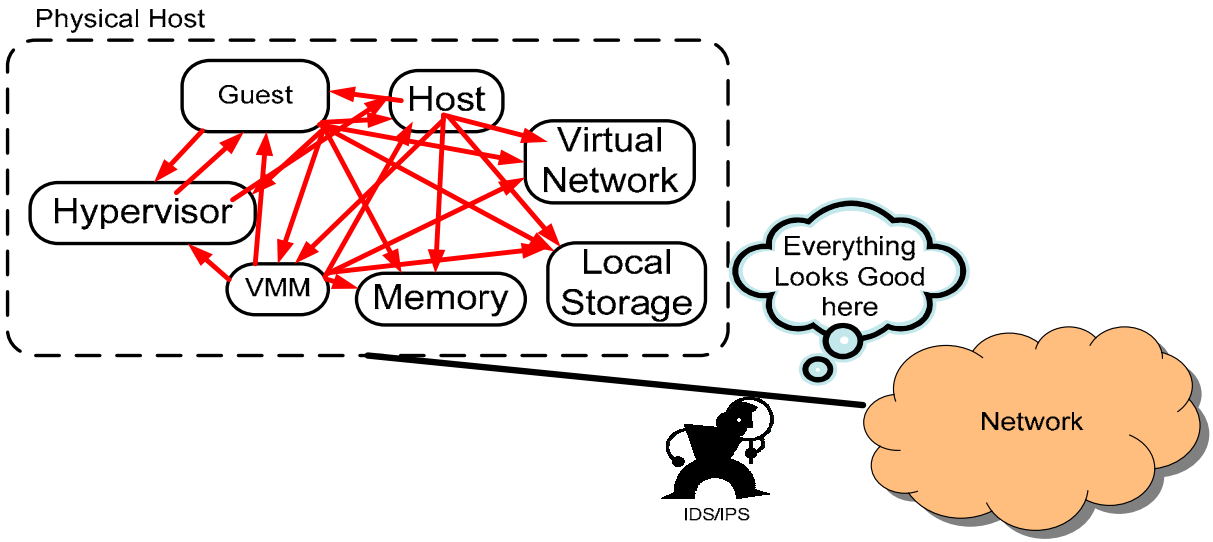
The Virtualization Challenge

- How does virtualization technology affect the definition of the scope?
- Virtualization affects
  - System boundaries
  - Network boundaries
  - Administrative boundaries
  - Monitoring effectiveness

The Virtualization System Model



The Virtual Attack & Monitoring Problem



Question: Virtual Boundaries

- Are virtual system boundaries equivalent to hardware system boundaries?
  - Depends on proper configuration
  - Depends on administrative model
  - Depends on what entities have access to application data, system configuration, network segments, and hypervisor
- Is cardholder data encrypted/protected appropriately?
  - How does it move?
  - Is it deleted when a system image moves from one virtual environment to another?

Virtual Networks and Configurations

- Are networking requirements, particularly firewalls, implemented in the virtual network?
  - If a DMZ is required in the virtual environment, firewalls need to be implemented
  - Network monitoring needs to deal with real and virtual networks
- Are configurations hardened appropriately according a set of standards?
  - Like hardware, virtual devices and systems need to be configured according to a set of standards

Monitoring, Access Control, & Testing

- Are configurations monitored in the virtual environment?
  - Virtual devices need to be monitored for unauthorized changes
- Is administrative access controlled and monitored according to PCI?
  - Privileges must be established for access to each level of abstraction
  - Logs and audit trails captured?
- Is testing conducted according to regulatory requirements?
  - Application vulnerability testing and scanning needs to take place
  - Are systems

Vulnerabilities and Accountability

- Vulnerability management
  - Multiple levels of vulnerabilities in the same system
    - Hypervisor
    - System software
    - Network and virtual network devices
    - Applications
- Logging and audit trails
  - Multiple levels of audit trails
  - Tight controls on audit trails

Identity & Access Management

- Virtualization provides challenges in defining access controls
- Separation of duties must be accomplished within systems rather than across devices
- This puts pressure on identity and access management systems
- Need to ensure that roles are defined appropriately in each virtual environment
- Need to have appropriate checks, balances, and workflow to support creation, modification, and certification of rights/accounts

Virtualization Boundaries

- Establish hardware boundaries that correspond to environment boundaries
  - Don’t mix zones in a single virtual environment
  - E.g., don’t put your DMZ and your internal network in the same virtual environment
- Use hardware networking where possible to define boundaries
- Tightly control accounts to virtual systems
- Ensure data is obscured when images are moved

Virtualization Administration

- No shortcuts for configuration, networking, and monitoring
- Separate responsibilities for system and virtual system administration
- Ensure that development and test do not use production images and data
- Develop strict configuration standards for all virtual systems
- Develop detailed procedures for instantiation and administration
- Monitor configurations of virtual systems as you would hardware

Cloud Computing and Compliance

- Cloud computing brings with it a larger set of issues
- The cloud's boundaries are loosely defined
- Cloud systems are recycled without the owner's control
  - Memory contents
  - Relationship to other systems
- Cloud providers do not provide the requisite guarantees needed to meet PCI compliance
  - Administrative access and processes
- Watch this space, but it's unlikely that you can convince a QSA that you can achieve compliance in a cloud today

Testing

- PCI requires several types of testing
  - Quarterly ASV scans of all external IP addresses
  - Internal scans
  - Application vulnerability analysis
  - Code review (or application firewall)
- HIPAA refers to testing
  - Testing of contingency plans
  - Penetration testing (if deemed appropriate) must be conducted with approval of management
  - NIST guidance suggests tests of authentication methods and auditing

Encryption

- PCI establishes clear guidance on encryption
  - Cardholder data (PANs)
  - Passwords/authentication data
- MA Law establishes rules
  - Transmission of PII on public networks
  - Encryption on laptops and portable devices
  - No statement regarding archived backups
- HIPAA provides guidance
  - Encryption is addressable buy not required
  - Based on results of risk assessment and must be considered “reasonable and appropriate”

Summary

- Changes occur all the time
  - New regulations
  - Technology adoption
  - Interpretation of regulations with new technology
- Know the requirements
  - Establish appropriate contracts with service providers
  - Ensure required testing
  - Deploy encryption where necessary
- Assemble a good argument for compliance
- Document, document, document