Top 5 PCI Compliance Challenges

Presenters:
Tim Sills, Senior Consultant, PCI QSA
Anton Abaya, Senior Consultant, PCI QSA
Tim Sills – PCI Background

• Experience with Visa’s Cardholder Information Security Program (CISP)
• Payment Card Industry (PCI) Qualified Security Assessor (QSA) since 2005
• Customers include retail organizations (brick & mortar and ecommerce), finance and banking institutions, health care providers, hosting companies, and service providers
Accudata’s Assessment Methodology

• Pragmatic approach
• Continually focused on the spirit of controls
• Willing to provide guidance on how best to address gaps
• Utilize tools to streamline collection and communication of data
Without segmentation and network isolation, the entire network may be in scope
Issue

• Meet compliance in shortest amount of time at minimal cost

Challenge

• Large, distributed environment with many control gaps
**USE CASE — CLOTHING RETAIL CHAIN**

**PCI ENVIRONMENT**

**Issue**
- Meet compliance in shortest amount of time at minimal cost

**Challenge**
- Large, distributed environment with many control gaps

**Solution**
- Implemented point to point encryption (P2PE) to remove cardholder data from environment and significantly reduce scope
Issue – Vulnerability Management

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

While it is acceptable for an assessor to sample business facilities/system components as part of their review of an entity’s PCI DSS compliance, it is not acceptable for an entity to apply PCI DSS requirements to only a sample of their environment (for example, requirements for quarterly vulnerability scans apply to all system components). Similarly, it is not acceptable for an assessor to only review a sample of PCI DSS requirements for compliance.

• Vulnerability identification and mitigation applies to the whole environment
**Issue**

- Call center workstations with legacy operating systems

**Challenge**

- Forklift upgrade and limited IT budget
**Issue**

- Call center workstations with legacy operating systems

**Challenge**

- Forklift upgrade and limited IT budget

**Solution**

- Developed endpoint security solution that provided application whitelisting, host-based firewall, and host-based intrusion prevention
Issue – Patch Management

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

• All systems and devices need to be maintained
• Multi-platform environments increase complexity
USE CASE — HEALTHCARE ORGANIZATION

Issue
- Apply system patches across distributed environment
- Install antivirus

Challenge
- Patch hundreds of devices
- Address multiple control gaps

©Accudata Systems, Inc. 2016
**Issue**
- Apply system patches across distributed environment
- Install antivirus

**Challenge**
- Patch hundreds of devices
- Address multiple control gaps

**Solution**
- Replaced workstations with Wyse thin clients
Issue – Logging and Monitoring

- Overwhelming amount of data to analyze
- Log data from multiple platforms
- Need for daily review of security events

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something goes wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.
**USE CASE — RETAIL MERCHANT**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect, normalize, and perform daily event log reviews</td>
<td>Limited IT resources to properly perform daily log review</td>
</tr>
</tbody>
</table>
**Issue**

- Collect, normalize, and perform daily event log reviews

**Challenge**

- Limited IT resources to properly perform daily log review

**Solution**

- Leveraged an outsourced security information and event management (SIEM) solution that includes daily event monitoring
**Issue – System Hardening**

<table>
<thead>
<tr>
<th>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.</td>
</tr>
</tbody>
</table>

- Hardening applies to all platforms
- Disable support for insecure services
USE CASE – PCI SERVICE PROVIDER

- Inconsistent system builds
- No established system deployment processes
**Use Case — PCI Service Provider**

**Issue**
- Inconsistent system builds

**Challenge**
- No established system deployment processes

**Solution**
- Established system hardening baselines
- Integrated with new image process
- Verified with configuration software that is integrated with vulnerability management
Top 5 Challenges Summary

- PCI Scope
- Vulnerability Management
- Patch Management
- Logging and Monitoring
- System Hardening
Got questions?
Our QSAs have the answers.
Accudata Offers a Full Suite of PCI Services:
Readiness, Guidance, and Remediation
Quarterly Scanning and Penetration Testing
Risk Assessment
PCI Attestation

Send questions or request a meeting with one of our QSAs: AskOurQSA@AccudataSystems.com