Crowe Horwath

February 2015

Ready for PCI DSS v. 3.0? Tips for Effective Compliance

Meeting the New Requirements for Scoping, Segmentation, and Threat and Vulnerability Management

By Angela K. Hipsher, CISA, QSA, and Craig D. Sullivan, CPA, CISA, QSA

PCI version 3.0 represents the newest updates made to the Payment Card Industry Data Security Standard (PCI DSS) established by the PCI Security Standards Council (PCI SSC).[1] Since PCI DSS v. 3.0 went into effect on Jan. 1, 2015, organizations that store, process, or transmit cardholder data now have a number of new or modified requirements to meet. To comply with these mandates and prepare for annual assessments by quality security assessors (QSAs), organizations need to review how they use network segmentation to establish security boundaries, not only to protect their systems but also to minimize the compliance burden and reduce the scope of the assessment. Those using segmentation now have more requirements for validating that segmentation.

Some of the noteworthy differences between PCI DSS v. 2.0 and PCI DSS v. 3.0 involve two areas of IT security:

1. **Compliance assessment scoping and network segmentation.** Under PCI 3.0, security requirements apply to all system components included in *or connected to* the cardholder data environment (CDE), that portion of a network that stores, processes, or transmits cardholder information. Independent assessors must understand how organizations conducted their assessments to define the assessment scope for compliance, or boundaries, of the CDE. In addition, assessors must validate the accuracy of the scope that management defined and documented. New requirements to prove the effectiveness of network segmentation through penetration testing are also in place.
2. **Threat and vulnerability management.** Recent high-profile breaches of cardholder data have led the PCI SSC to step up the number of controls organizations employ in maintaining anti-virus protection, installing software patches, and conducting vulnerability scans and penetration tests.

Scoping and Segmentation

In an environment where cyberattacks targeting consumers' personal financial information are on the rise, it's not enough to secure only the core systems of the CDE. Organizations also must examine and protect the attached and support systems that define and defend the CDE.

Attached and Supporting Systems

The scope of PCI DSS v. 3.0 includes not only the networked systems and infrastructure that handle cardholder data – that is, the CDE itself – but also the systems that attach to or support the infrastructure of the CDE:

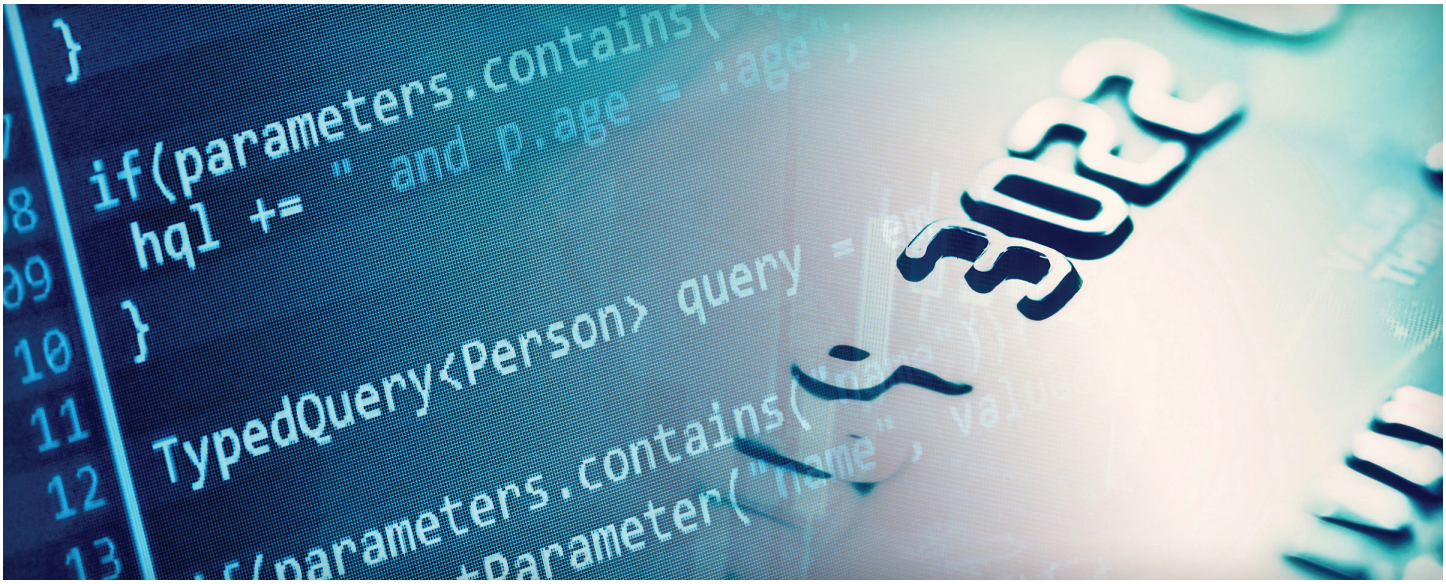
- **Attached systems communicate with systems in the CDE.** These are systems of record that might not store cardholder data but might receive transaction information from the systems that are handling cardholder data, such as enterprise resource planning (ERP) systems, billing systems, and data warehouses.
- **Supporting systems connect to the CDE.** These might not actually sit in the CDE because they might manage and regulate the entire network, including the segment known as the CDE. Active directory servers that manage authentication for the network, central log servers, and anti-virus consoles are examples of supporting systems.

Any system that needs to have access to both the CDE and the rest of the network is a connected or supporting system that must be considered in scope for the annual PCI compliance review. As a rule of thumb, if a system can affect the security of cardholder data, it is considered to be in scope.

New Scoping Requirements

PCI DSS v. 3.0 contains several new requirements that affect and assist in determining and documenting the scope for the compliance assessment.

1. **Requirement 1.1.3.** Organizations must maintain a current diagram showing how cardholder data flows through their systems.
2. **Requirement 2.4.** Organizations have to maintain an inventory of the system hardware and software that is considered in scope.
3. **Requirement 9.9.1.** Organizations must maintain an up-to-date list of devices.
4. **Requirement 11.1.1.** Organizations have to conduct an inventory of all authorized wireless access points and justify why those access points are part of the inventory.



All four of these requirements are designed to help organizations go beyond traditional security practices by focusing on data flow and paying more attention to connected and supporting systems.

To comply with these requirements, it can be helpful for an organization to start by surveying employees about how they receive data, which systems they draw data from or push data to, and whether any third-party vendors move data in and out of the environment.

Network Architecture and PCI Scope

How a network is structured can affect scope under PCI DSS v. 3.0. A simple, or "flat," network that has no virtual local area networks to separate systems allows malware, viruses, and targeted attacks to spread throughout the computing environment. To mitigate such threats, organizations can use segmentation to create compartments within the network.

Effective segmentation must go beyond traditional zone definition. Network traffic from PCI-related zones to unrelated systems and zones should be blocked or restricted, and allowable traffic should be limited to specific IP address routing on specific protocols and ports required for business purposes. Segmented support systems, such as logging systems, should still be considered in scope where the support systems have a direct impact on the security and compliance of the primary systems in the CDE.

Organizations conduct penetration tests to measure the effectiveness of their IT defenses. PCI DSS v. 3.0 contains a new requirement for validating segmentation through penetration testing:

- **Requirement 11.3.4.** If an organization employs segmentation to isolate the CDE from other networks, the penetration test needs to verify that the segmentation methods are operational and effective.

The test should also consider operational controls that could affect the ability to bypass the segmentation. Practices like sharing or reusing user IDs and passwords across different network segments or systems could invalidate the segmentation if those credentials have been compromised on a noncompliant segment of the network.

Threat and Vulnerability Management

PCI DSS v. 3.0 also introduces several new requirements, or clarifies existing requirements, to strengthen threat and vulnerability management. Specific areas of focus include employing appropriate anti-virus software, conducting vulnerability scans and penetration tests, and installing corrective software patches.[2]

Anti-virus Software

PCI v. 2.0 required organizations to evaluate evolving malware threats, but it provided an out on implementing anti-virus software on systems not commonly affected by viruses. PCI DSS v. 3.0 introduces two important changes affecting anti-virus software:

1. **Requirement 5.1.2.** This new requirement obligates organizations to evaluate evolving malware threats for systems that are not commonly affected by malicious software on an ongoing basis. Organizations will need to stay current with industry trends in emerging malicious software and its possible effect on their systems.
2. **Requirement 5.3.** Under this requirement, anti-virus solutions must be actively running and – as previously mandated by requirement 5.2 of PCI DSS v. 2.0 – cannot be disabled or altered by users unless specifically authorized by management on a per-case basis.

Organizations should consult their anti-virus software vendors for assistance with updating their IT security policies to include procedures for enhanced security controls related to anti-virus solutions.

Vulnerability Scans and Penetration Tests

Vulnerability scanning and penetration testing are two techniques organizations can use to help identify weaknesses in security controls meant to protect their CDEs. Vulnerability scans sweep across computer systems to detect potential areas of weakness, and penetration tests simulate attacks that intruders might employ by taking advantage of vulnerabilities they can exploit, capturing credentials, and escalating rights.[3] PCI DSS v. 3.0 introduces a new requirement for penetration testing:

- **Requirement 11.3.** Under this requirement, which goes into effect July 1, 2015, organizations must develop and implement a methodology for penetration testing. Until that time, organizations must continue to follow the penetration testing requirements of PCI DSS v. 2.0.

Although vulnerability scans must be conducted by independent vendors approved by the PCI SSC, organizations are allowed to conduct their own penetration tests. If they do perform their own penetration tests, testers must be qualified and independent – in other words, administrators of the system cannot do the testing. To meet the new requirement, organizations must clearly document the scope, tools, approach, and results of their internal tests.

Corrective Software Patches

Under PCI v. 2.0, organizations have been required to install critical security patches within 30 days of being released, and PCI DSS v. 3.0 clarifications strengthen this requirement:

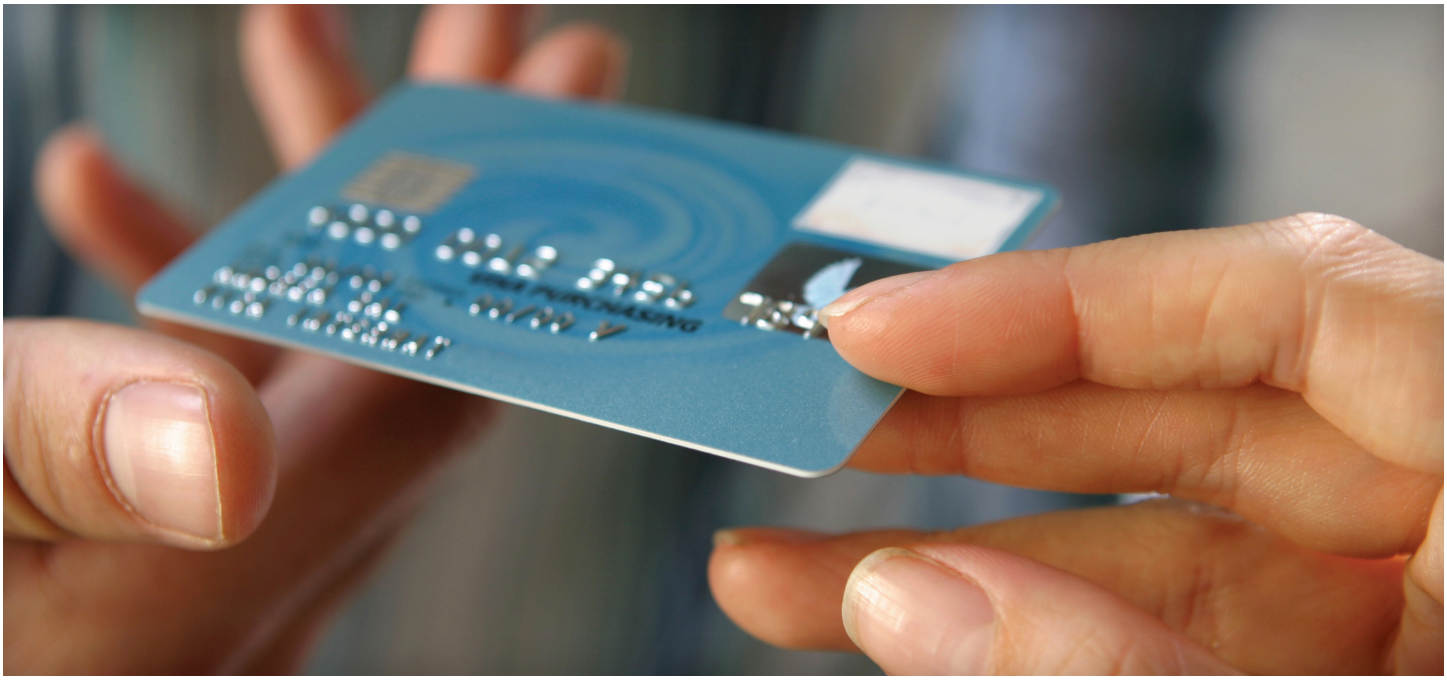
- **Requirement 6.2.** In addition to installing critical security patches within 30 days, organizations must also install all noncritical vendor-supplied security patches within a time frame established by the organization's policy.

During their examinations, QSAs will check that organizations are adhering to their own policies for updating both critical and noncritical software patches. Policies should clearly document an acceptable time frame, as determined by management, for implementing all patches.

Primary Steps to Take

In light of technology changes and a standard that evolves over time, obtaining and maintaining compliance with the PCI DSS is not easy. Every organization should keep in mind the primary steps in the journey to compliance, which include the following:

- Reviewing new software solutions, vendors, and programs will be imperative to maintaining ongoing compliance.
- Understanding that new technologies and even minor changes in IT architecture could affect compliance. For example, adding wireless access points or opening a firewall port could nullify network segmentation.
- Using vulnerability management programs to maintain compliance and also to understand and manage risks on a daily basis.
- Recognizing new challenges to achieving compliance with the new version of the standard early will be the key to ongoing success with the QSA.
- Maintaining appropriate logging and monitoring controls, along with an effective incident response plan, is important for managing risk and compliance.
- Working with a QSA to understand all aspects of the scoping process and using new requirements for inventory, effective segmentation, and penetration testing will facilitate the compliance assessment.



Taking these steps toward complying with PCI DSS v. 3.0 can help merchants, service providers, third-party vendors, and other organizations that store, process, or transmit cardholder data to mitigate the potential for a cyberattack that results in cardholder data theft and misuse.

---

[3] PCI SSC, "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures" Version 3.0, November 2013, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf Note that this article cannot cover every change brought about by PCI v. 3.0, and organizations should be sure to review those not covered as well as those discussed in this article.

[4] For more information about assessing and managing vulnerabilities, see Angie Hipsher, Craig Sullivan, and Brian Wang, "PCI DSS Vulnerability Assessments: Going Beyond Patch Management," Crowe Horwath LLP, November 2013, http://www.crowehorwath.com/ContentDetails.aspx?id=7497

[5] For more information about vulnerability scans and penetration tests, see Raj Chaudhary and Christopher R. Wilkinson, " The Pros and Cons of Vulnerability Assessments and Penetration Tests," Crowe Horwath LLP, April 2014, http://www.crowehorwath.com/folio-pdf/TheProsandConsofVulnerabilityAssessments_RISK14956.pdf

Contact Information

Angie Hipsher is with Crowe Horwath LLP in the Indianapolis office. She can be reached at 317.208.2430 or angie.hipsher@crowehorwath.com.

Craig Sullivan is a partner with Crowe in the South Bend, Ind., office. He can be reached at 574.236.7618 or craig.sullivan@crowehorwath.com.

"What Your QSA Should be Clarifying About Version 3.0," a recording of a Nov. 19, 2014, Crowe webinar presentation by Angie Hipsher and Craig Sullivan, is available at: http://www.crowehorwath.com/ContentDetails.aspx?id=10026