February 12, 2019

# Better Understanding PCI Penetration Testing Requirements

CYBERSECURITY, DIGITAL & TECHNOLOGY, RETAIL
BY SCHNEIDER DOWNS PROFESSIONAL

If your company takes credit cards, you may be wondering if you are required to have a penetration test. In the past, it had been voluntary, but with PCI DSS version 3.0 and on, there are specific penetration testing requirements, depending on what self-assessment questionnaires (SAQS) category you fall into. The actual requirements vary based upon the number of transactions in a given year and how they are performed. For some organizations, yearly penetration testing is required, while others don't require it at all. In this article, we discuss: why you need to be compliant, in what scenarios penetration testing is required, what that testing should cover and how to get the best value for your money in a PCI penetration test. This is also a good reference for penetration testers looking to perform PCI penetration testing. Keep in mind that all organizations that accept payment via credit card must be compliant with the Payment Card Industry Data Security Standards (PCI DSS).

Compliance is expensive and monotonous-- why should I be PCI-compliant? According to the official PCI website, some of the liabilities for not being compliant are: the cost of reissuing new credit cards, legal fees and removal of the ability to accept payment cards. Any one of these consequences can be costly. Not only that, but the PCI DDS requirements are actually good security practices to follow for any company, even those that do not require PCI compliance, so there is little reason not to adhere to them.

If you are not sure what SAQ category your organization falls into, your bank or payment processor should be able to tell you, since they are the parties that receive the SAQ and other PCI DSS documentation. You can find more information on SAQs and their descriptions here. As far as penetration testing goes, SAQ A-EP, D Merchants and D service providers all require penetration testing. Organizations that are SAQ B-IP, C-VT and C require penetration testing if the cardholder data environment (CDE) is separated from the rest of the network using segmentation. An example of segmentation would be that the CDE network uses some of the same networking gear as the rest of the network, but is isolated using VLANs, firewall rules and/or access control lists (ACLs). If that is the case, you may need to have penetration testing performed. Below is a matrix that breaks down the penetration testing and vulnerability scanning requirements by SAQ:

**Vulnerability Scanning and Penetration Testing Requirements**

| SAQ | A | A-EP | B | B-IP | C-VT | C | P2PE-HW | D Merchant | D Service Provider |
|---|---|---|---|---|---|---|---|---|---|
| Quarterly External Vulnerability Scans (ASV) | No | Yes | No | Yes | No | Yes | No | Yes | Yes |
| Quarterly Internal Vulnerability Scans | No | Yes | No | No | No | Yes | No | Yes | Yes |
| Penetration Testing | No | Yes | No | * | * | * | No | Yes | Yes |

*Only required if segmentation is used to isolate CDE from other networks.

For those organizations that do require a penetration test, you may wonder what all should be covered. At a high level, a PCI penetration test should be performed using techniques favored by real attackers in an effort to actually compromise the cardholder data environment. A penetration test cannot consist of a vulnerability scan alone; actual exploitation must be attempted. The test should have the PCI network as the main objective. If segmentation is in use to isolate the cardholder environment, that control must also be verified as being effective as part of the testing.

Here are some tips for how to get the best value out of your PCI penetration test. The most important is to ensure that you are working with a competent penetration testing provider. The best way to do this is to evaluate a number of vendors against a couple key areas. There are three items you want to look at. First, verify the firm is familiar with the PCI DSS penetration testing requirements and that they can explain how they fulfill those testing needs. Second, ask for and talk to references who have used their services before for similar types of testing.  Lastly, review an example penetration test report from the firm. If the report does not provide clear and concise findings and recommendations, is padded with dozens or hundreds of pages of vulnerability scan results, or is difficult to comprehend, then look elsewhere.

Once you have a list of potential providers, consider the scope of the penetration test. Oftentimes, we see clients doing barebones testing that does what PCI testing requires and nothing else, which may exclude large sections of your organization's network and give you a false sense of security. Talk with your penetration testing provider to see what the additional cost is to do a full-scale test that not only tests the PCI environment properly, but also checks for common issues on the rest of your network. It may not cost much more to have a more comprehensive penetration test, which will give you a more complete profile of the risk on your network, not just the cardholder data environment.

If you have any questions or are interested in Schneider Down's services, feel free to contact a member of our sales or cybersecurity team.

**References**

https://www.pcisecuritystandards.org/

Jeff Man (Jan  8th , 2019). Skype interview.

## You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.