PCI DSS v. 3.2: New Requirements Coming to Protect Your Customers' Wallets

PCI Council announces that new requirements will be considered "best practices" until compliance becomes mandatory on February 1, 2018

By Courtney K. Stout and Bryan Thompson

The Payment Card Industry (PCI) Security Standards Council (PCI Council) released Version 3.2 of the PCI Data Security Standard (PCI DSS), containing several new requirements for merchants, acquirers, and other entities that accept, transmit or store cardholder data in order to protect customer payment card information. The new release focuses on mitigating current vulnerabilities identified in data breach reports, including those presented by third party service providers, authentication protocols, and outdated encryption. The changes are also intended to help companies maintain and effectively test compliance between annual PCI assessments.

PCI DSS V. 3.2 FOCUSES ON VULNERABILITIES IDENTIFIED IN BREACH REPORTS

Results from the Ponemon Institute 2014 Security & Compliance Trends in Innovative Electronic Payments survey, and the 2016 Verizon Data Incident Report.

The PCI DSS Version 3.2 (*agreement required*) is now available for use, and will **officially replace** the current PCI DSS Version 3.1 **on October 31, 2016**. Accordingly, all PCI DSS assessments taken on or after November 1 must evaluate compliance against Version 3.2. However, the new requirements contained in the latest version will be **considered "best practices" until February 1, 2018** to give entities enough time to implement necessary changes and come into compliance. Consequently, February 1, 2018 is the mandatory deadline for companies contractually required to be "PCI compliant" to review and change their security practices and procedures to ensure compliance with the new requirements and avoid fines, fees, and other assessments.

What's New in PCI DSS v.3.2?

Multi-Factor Authentication

Companies will soon be required to use **multi-factor authentication** for administrative access to the cardholder data environment.

Version 3.2 includes some important changes to the present standard, including **requiring multi-factor authentication** for **all non-console administrative access** to the cardholder data environment. Multi-factor authentication requires the use of two or more credentials to authorize a person's access to card data and systems. Different authentication factors include (i) something you know - such as a password; (ii) something you have - such as a token or device code; or (iii) something you are - such as biometric data like a fingerprint.

> "The PCI DSS defines "non-console access" as "logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external, or remote, networks."

Under the prior release, the PCI DSS only required "two-factor" authentication for any **remote** access into the cardholder data environment. Version 3.2 adds the requirement that all "non-console" administrative access, even when accessed by an employee from the company's internal network, must employ multi-factor authentication. Thus, anyone that has "administrative access" rights will need to use multi-factor authentication to access the cardholder data environment.

> **"Administrative Access"** is defined as "elevated or increased privileges granted to an account in order for that account to manage systems, networks and/or applications."

While two-factor authentication is considered a type of multi-factor authentication, the PCI Council's standard under Version 3.2 requires that a company must use a *minimum* of two credentials. Additionally, the PCI Council cautions that using one authentication method twice – for instance, requiring users to provide two separate passwords – does not count as multi-factor authentication under PCI DSS. Companies should verify that their authentication protocols meet the PCI Council's multi-factor standard.

Service Provider Requirements

Version 3.2 contains several **new requirements for service providers**, including consolidating and integrating existing criteria for additional assessments for certain service providers.

Version 3.2 integrates the PCI Designated Entities Supplemental Evaluation (DESV) – previously a stand-alone document – into the PCI DSS at Appendix A3. The DESV is a set of validation requirements intended to help service providers and others address identified challenges and adopt ongoing security efforts to protect payment data. Although these supplemental validation requirements for service providers do go above and beyond the standard PCI DSS requirements, Troy Leach, PCI Security Standards Chief Technology Officer, clarifies that many are simply extensions of "existing PCI DSS requirements that should be demonstratively tested more regularly, or require more evidence that the control is in place." Additionally, even though the DESV is now integrated into the PCI DSS, **an entity is only required to be assessed under the DESV requirements if an acquirer or a payment brand specifically instructs a service provider to do so**. Key requirements include measures for their own effective compliance program oversight, correct scoping of the PCI environment, and placing effective mechanisms to allow a company to detect and trigger alerts for failures in critical security controls.

Since service providers are an integral part of securing cardholder data, and third parties have been identified as a weak link in data breach reports, Version 3.2 also adds a number of significant changes requiring **service providers to**:

- Maintain documented description of cryptographic architecture, including details of all algorithms, protocols, and keys for the protection of cardholder data (Req. 3.5.1);
- Implement processes to timely detect, report and respond to failures of critical security control systems, including, but not limited to, failures of firewalls, anti-virus, physical and logical access controls, audit logging mechanisms, and segmented controls (if used) (Req. 10.8);
- Confirm PCI DSS scope by conducting penetration testing at least every six months and after any change to segmentation controls or methods (Req. 11.3.4.1);
- Engage executive management in establishing responsibility for the protection of cardholder data and PCI DSS compliance program (Req. 12.4.1); and
- Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures, including daily log reviews; firewall rule-set reviews; applying configurations to new systems; responding to security alerts and to changes in management processes (Req. 12.11).

Changes to the Cardholder Data Environment

Companies will need to apply the PCI DSS requirements whenever modifications are made to their in-scope networks and systems.

Organizations must ensure that **all *relevant* PCI DSS requirements** are implemented whenever there is a "significant change" in the cardholder data environment (Req. 6.4.6), which should already be a part of a company's activities to maintain PCI DSS compliance. This requirement is meant to address the compliance gap that may occur between annual PCI DSS assessments. Due to changes to in-scope systems throughout the year, the compliance status of the environment at the time of a breach may differ from that at the last PCI DSS assessment.

Masking and Encryption

Version 3.2 includes additional changes, such as extending the sunset date for using Secure Sockets Layer (SSL) and early Transport Layer Security (TLS) to **June 30, 2018** for some companies, and clarifies that companies must "mask" payment card primary account numbers (PANs) longer than the first six/last four digits unless there is a legitimate business need.

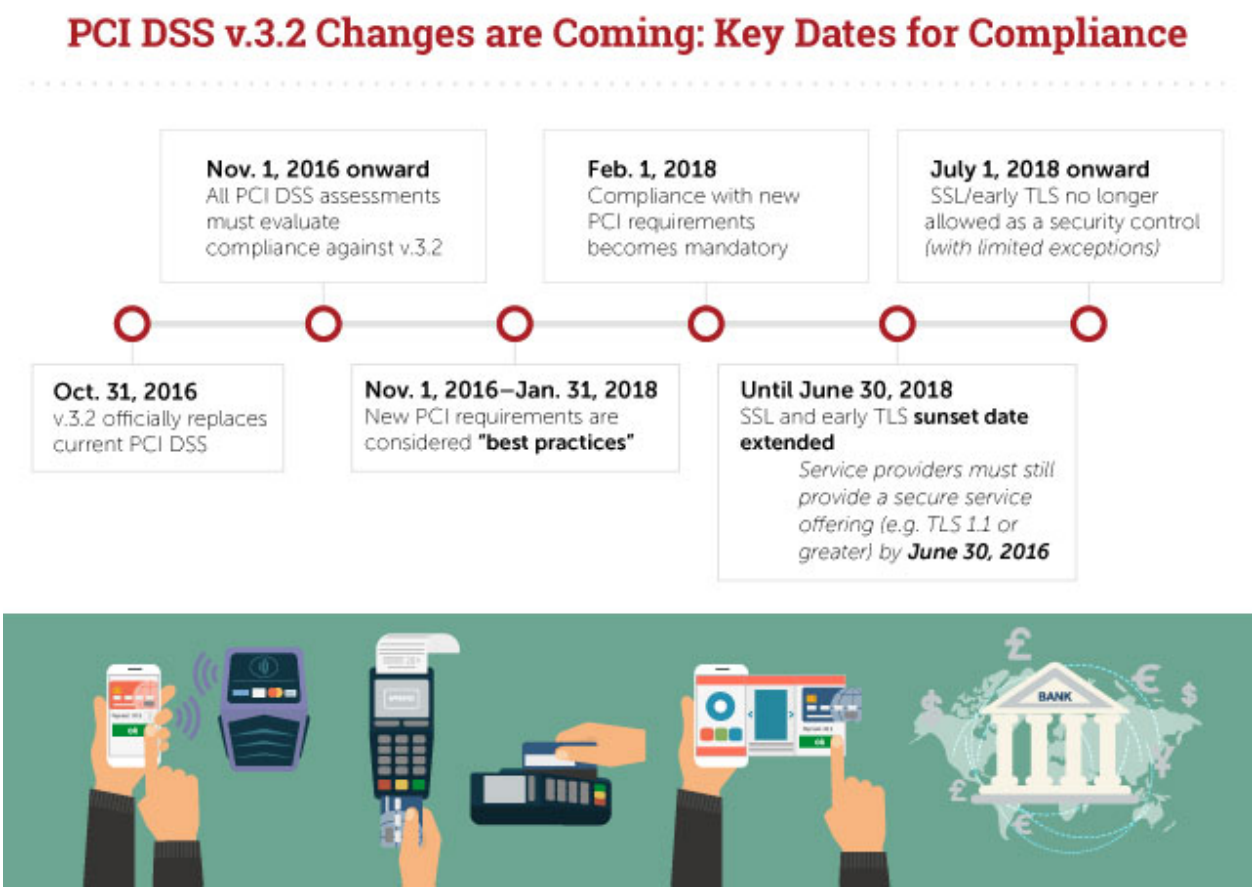
- **SSL/early TLS sunset extended.** Although previously announced, the PCI Council formally delays one significant deadline in Version 3.2 by **extending the SSL and early Transport Layer Security (TLS) sunset date** set by Version 3.1 from June 30, 2016, **to June 30, 2018**, giving an additional two years to migrate away from these popular-but-outdated encryption standards. If your company is still using these now-outdated encryption methods, you are required to prepare a formal "Risk Mitigation and Migration Plan" in the interim. However, it is recommended that your company move from these encryption protocols as soon as possible; as we have noted previously, SSL and early TLS do not meet the PCI's mandatory requirements for strong encryption.

  If you are a **service provider**, your company **must still provide a secure service offering** (such as TLS 1.1 or greater) **by June 30, 2016**, under Appendix A2 to the new version.

- **"Masking" PANs**. Version 3.2 clarifies the existing requirement to "mask" payment card account numbers (PANs) so as to only display, at most, the first six and the last four digits and advises companies to ensure that "only the minimum number of digits is displayed" to perform a specific business function. The prior version simply stated that personnel with a **legitimate business need** may see *the full* PAN, while Version 3.2 clarifies that there must be a legitimate business need to view PANs longer than the first six/last four digits (Req. 3.3 and related guidance).

Key Dates for Compliance

Though Version 3.2 will become official as of October 31, 2016, most changes will not go into effect immediately in order to give covered businesses time to adjust to the new requirements. Your company should be aware of the following deadlines to ensure that its transition to Version 3.2 meets the PCI Council's transition timetable.



The Takeaways

Exploiting data security weaknesses in payment card systems and networks to steal and monetize cardholder data remains a popular tactic for cyber thieves. The update to the PCI DSS is, as the PCI Council admits, to ensure that the payment card industry is both guarding against old threats to the security of consumers' payment card information and addressing new vulnerabilities that continue to emerge.

Securing payment card systems is important for both traditional brick-and-mortar merchants as well as the new and innovative payment methods that have emerged in recent years, such as e-commerce enterprises and mobile payments via smartphones and other devices. With these new technologies, the payment card industry and the merchants themselves have had to confront new and previously unforeseen vulnerabilities to the security of customer payment card information.

Non-service providers received a two-year reprieve from migrating away from SSL and early TLS, but should not procrastinate in implementing more secure encryption standards, given the known vulnerabilities in both of these legacy standards. Meanwhile, **service providers** still using SSL or early TLS will **need to act swiftly** to meet their **June 30, 2016 deadline to implement new encryption requirements**. Most of Version 3.2's new requirements will be "best practices" until February 1, 2018, which may seem far away today. However, some of the changes that may be required, such as negotiating new contracts or replacing authentication systems and processes, may take a considerable amount of time to implement. Companies should use this two-year window to review their security practices and make all necessary changes to guarantee their adherence once Version 3.2 goes live and avoid potential fines from the payment card brands for non-compliance.

The PCI Council has posted the new PCI DSS Version 3.2 and a summary of changes between Version 3.1 and 3.2 (*agreement required*), as well as a Resource Guide explaining the modifications that Version 3.2 brings. Companies should consult knowledgeable technology or legal counsel if they have any questions about this new standard or have questions about compliance.