**PCI DSS 3.2: What to Expect?**

PCI SSC releases new version of PCI DSS every two years ever since its inception. Following that schedule, the new version of PCI DSS was expected to be released in November this year. However, it is anticipated that the release will come a little earlier this time. The question is, why is it being released earlier? How much would it affect organizations and what changes will be brought to them as a result of this? The main reason is to aware merchants about TLS migration deadline extending from June 2016 to June 2018. Version 4.0 was not released as changes to the version were very minor. Therefore, version 3.2 will be released instead.

**What are the Expected Changes in PCI DSS 3.2?**

A confirmed change that will be a part of PCI DSS 3.2 is the formal increase in deadline for replacement of insecure SSL and early TLS with their secure current equivalents. In December 2015, the deadline was already announced to be extended to June 30, 2018.

The CTO of PCI Council, Troy Leach, in an interview on PCI SSC website, hinted at some potential changes that will be a part of PCI DSS 3.2. These include:

* Additional multi-factor authentication for administrators within a CDE i.e. Cardholder Data Environment
* Incorporation of some of Designated Entities Supplemental Validation (DESV) criteria for service providers
* Clarification of masking criteria for Primary Account Numbers (PAN), when displayed.

Now let us take a closer look at the changes expected to be a part of PCI DSS 3.2

1. **Increase in Deadline Date**

In earlier version of PCI DSS 3.1, the deadline for companies to migrate from SSL and early TLS to latest version of TLS was given as June 2016. Later, in November 2015, the deadline was extended to June 2018.

Many companies are still considering the previous deadline so as to avoid risks. SSL encryption can pose threat to information security of a business due to its easily exploitable vulnerabilities. Migrating to latest TLS as soon as possible would be the safest choice for many organizations.

1. **Additional Multi-Factor Authentication for Administrators within a CDE**

PCI DSS 3.2 will assess additional multi-factor authentication for administrators within a Cardholder Data Environment. Multi-Factor authentication, also called two-factor authentication, is one of the requirements of PCI DSS as it allows to effectively secure your cardholder data environment. For correct configuration of multi-factor authentication, you need to have at least two out of three factors in hand:

* Anything that you know e.g. your username or password, etc.
* Anything you have e.g. getting a code from phone
* Anything you are e.g. your fingerprints

Before PCI DSS 3.2, two-factor or multi-factor authentication was required only in case of access to network remotely by the employees, third parties and administrators. In 3.2, it is expected that multi-factor authentication needs to be done even if the access is taken within the CDE.

1. **Incorporation of Designated Entities Supplemental Validation (DESV) Criteria for Service Providers**

Some extra validation criteria may be incorporated by PCI DSS 3.2 for service providers. This means that even after PCI DSS validation, some entities chosen by payment brands or acquirers will be required to undergo extra validation to determine if they have achieved compliance in accordance to their daily practices or not. For example, extra validation could mean checking change controls list of a merchant in the past one year. Procedures showing day-to-day compliance could be checked such as mapping of suspicious events, documentation updates, etc.

1. **Clarification of masking criteria for Primary Account Numbers (PAN)**

PCI DSS 3.2 will also clarify masking criteria for Primary Account Numbers during display. Masking means to hide information from clear view and it is not the same as encrypted data. For example when you display your credit card number, you have to mask it. At the most, you can only show first six and last four numbers. Going beyond this requirement would deem you noncompliant. Masking criteria for PAN will be clearly identified in 3.2. Another important thing to note is that if your business stores Personal Account Numbers, you need to have a mechanism to encrypt and secure it.

**How to Prepare Yourself for PCI DSS 3.2?**

Although complete details of PCI DSS 3.2 are not in our knowledge yet, it would be better to stay up to date with the latest PCI DSS version to be able to adopt the changes easily. This would help save time and costs. To prepare for the best, organizations need to take time in evaluating their security investments. They need to continue to evaluate their payment acceptance procedures and have awareness about their organization’s inherent potential risks.

Since the SSL / Early TLS update in PCI DSS 3.2 was already announced in December 2015, organizations need to be already on the path to address the issue. To understand where to start with the migration process, they need to review the “Bulletin on Migrating from SSL and Early TLS”, which serves as a good resource for step by step guidance.

To prepare for additional multi-factor authentication, organizations need to review their current authentication system and how it is being managed in their cardholder data environment. Present roles of administrators should be reviewed and accessed for identifying where exactly will the changes have an impact once the new requirement is put into practice.

Service providers need to take steps to maintain documented description of cryptographic architecture, report on security control system failures, and set up roles and responsibilities to protect cardholder data and PCI Compliance program. Organizations that are not service providers still need to evaluate new requirements and check if implementing any of those security controls will provide benefit to the organization, even if it is not related to their compliance.

Stickman Consulting provides trusted IT security professional services to help you in achieving PCI DSS compliance by assessing your current compliance status and updating to the latest version 3.2. We can help you review the effect of the changes to organization-specific environment and to create a suitable action plan.