www.pwc.com

PCI DSS v3.2
Are you prepared?

pwc

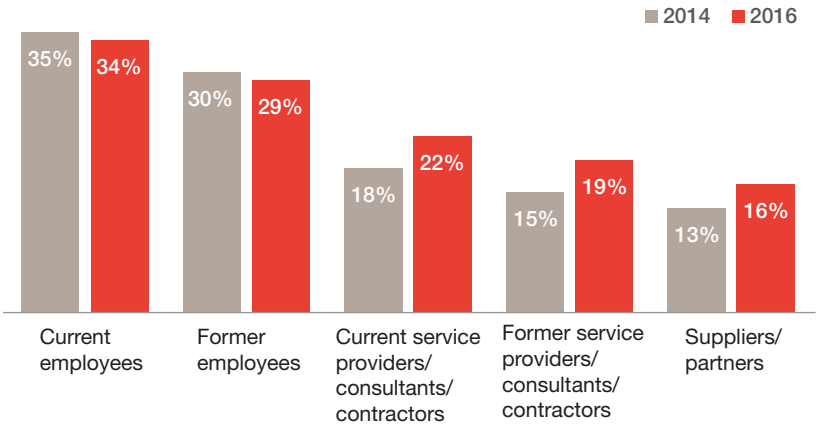
The Payment Card Industry Security Standards Council (PCI SSC) has published an update to the Payment Card Industry Data Security Standard (PCI DSS) in April 2016. The new version, 3.2, has replaced v3.1 with the intent of addressing changes to cyberspace and technology. With less than two months to go for this standard to come into effect, this publication delves into and deciphers the expectations of the council.

This version of the standard specifically targets 'service providers' with five new sub-requirements, along with the introduction of multi-factor authentication for all non-console administrative access and remote access. PCI SSC has also relaxed some timelines through this update.

It is unusual for of the council to release a new version of the standard early in the year. Our experience and the statistics gathered globally point to an increased and, to an extent, unaddressed risk of internal and third-party threats.

PwC's Global State of Information Security Survey (GSISS) 2016[1] points to a

22% increase in incidents attributed to business partners, with employees as the most cited source of compromise.



The new version (rightly) takes definite steps towards security in these areas. Also, in order to ensure that organisations get enough time to address the changes and subsequent challenges, v3.2 was released in April this year.

What should organisations expect?

EVEN THE MIGHTY WALLS OF TROY WERE RENDERED USELESS BY THE TROJAN HORSE, WHICH IS WHY A LAYERED DEFENSE STRATEGY WORKS BETTER WHEN IT COMES TO CYBER SECURITY.

An additional factor of authentication adds a strong layer of protection against brute-forcing, guessing and social engineering. Increased incidents of security breaches have made it important for organisations to implement this technology. A few high-profile cyberattack cases such as HBGary Federal could have been prevented by proper use of multi-factor authentication.[2]

The new requirements specifically targeting service providers increase the responsibilities of organisations who engage them. Organisations would now need to ensure that their service providers are maintaining cryptographic key architecture, documenting PCI DSS compliance responsibilities and sharing formal documents with them. In addition, organisations would now have to ensure that their service providers set up a reporting structure and mechanism to report failure of any critical security controls. New requirements for service providers can be utilised by organisations to ensure greater scrutiny of third parties engaged by them.

Changes in v3.2 in a nutshell

Annual trainings for software developers

Multi-factor authentication for privileged accesses

All significant changes to address applicable PCI DSS requirements

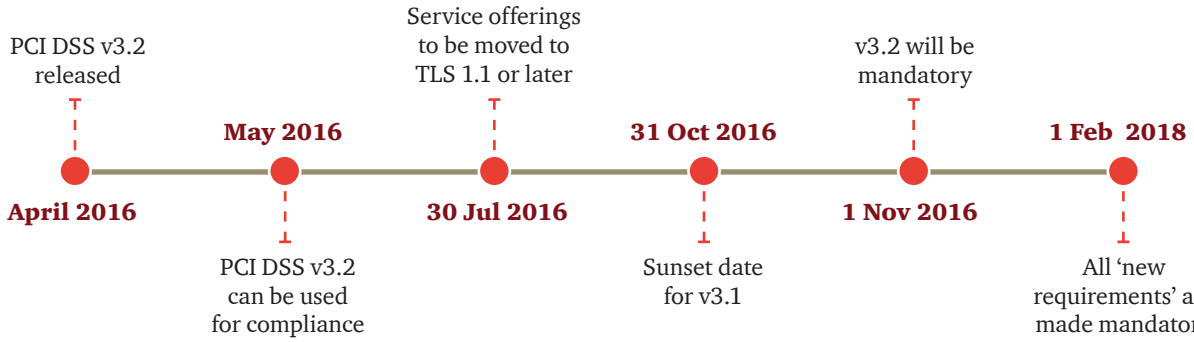
1. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
2. HBGary Federal's former CEO had administrative privileges on the company's Google mail exchange, and used the same password as that of his social platform accounts. Had a multi-factor control like 'Google Authenticator' been used for the company's privileged Google mail access, we believe that it would have made the attacker's job more difficult despite knowing/guessing/brute-forcing the password. This attack eventually led to HBGary Federal—a security company specialising in cyber security—being wiped out from existence.

What should service providers expect?

The new version of the standard has directly incorporated some requirements of the Designated Entities Supplemental Validation (DESV). While the rest of DESV has been added as an appendix to the standard, PCI SSC has left it to acquirers to mandate validation of the same.

SSC has relaxed the date for migrating to safer versions of Transport Layer Security (TLS) for all entities to 2018. However, service providers were required to ensure that their service offerings stop supporting Secure Sockets Layer (SSL) and Early TLS by 30 June 2016.

To ensure that the standard is not taken lightly as an annual compliance activity, the new version mandates that certain security practices be carried out regularly throughout the year by service providers, and that they provide additional assurance about their security measures.



Changes and important deadlines

PCI DSS v3.2 comes with around 47 clarifications on requirements, three additional guidance notes on existing requirements and about eight new/evolved requirements. Clarifications like inclusion of a service description for the service provider list maintained as part of requirement 12.8 are intended to make the intent of the requirement clear. The clarifications and additional guidance come into effect immediately.

Although the sunset date for the older version (3.1) of the standard is set to 31 October 2016, the council has provisioned for some extended deadlines for a few of its requirements.

No.	Requirement
3.5.1	New requirement for service providers to document and maintain cryptographic architecture
10.8	New requirement for service providers to detect and report on failures of critical security control systems
11.3.4.1	New requirement for service providers to perform penetration testing of segmentation controls biannually
12.4	New requirement for service provider's executive management to document and establish responsibilities towards cardholder data protection and PCI DSS compliance
12.11	New requirement for service providers to perform quarterly reviews of security policies and operational procedures implementation

Conclusion

At the core of the changes are the four areas the council aims to address:

- Increased focus on service provider compliance
- Additional layer of access control for privileged access to cardholder data environment
- Scrutinising of changes for causal effects on PCI controls/scope
- Requirement of cryptographic architecture for all encryption requirements

In our opinion, the relaxation of deadlines by PCI SSC, although it provides a breather to security strategists and key stakeholders across organisations, does not lessen the effort required to achieve these objectives. Organisations will still continue to face challenges like inability to switch to TLS 1.1 or above due to dependency on the application architecture components, dearth of investments required to bring in technology for better compliance management and lack of consistent focus on PCI compliance activities.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,23,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

Contacts

Sivarama Krishnan
Leader, Cyber Security
sivarama.krishnan@in.pwc.com
+919650788787

Siddharth Vishwanath
Partner, Cyber Security
siddharth.vishwanath@in.pwc.com
+91 (22) 6669 1559, +91 9167190944

Murali Talasila
Partner, Cyber Security
murali.talasila@in.pwc.com
+91 40 44246721, +91 9958439996

Hemant Arora
Executive Director, Cyber Security
hemant.arora@in.pwc.com
+91 (124) 626 6717, +91 9711559686

Sundareshwar Krishnamurthy
Partner, Cyber Security
sundareshwar.krishnamurthy@in.pwc.com
+919930105282

Manu Dwivedi
Partner, Cyber Security
manu.dwivedi@in.pwc.com
+91 (0) 80 4079 7027, +91 9611114377

PVS Murthy
Executive Director, Cyber Security
pvs.murthy@in.pwc.com
+91 (22) 66691214, +91 9867743050

Paras G Arora
Associate Director, Cyber Security
paras.g.arora@in.pwc.com
+919560911644

pwc.in

Data Classification: DC0

MJ/September2016-7455