Clearing the Cloud Over PCI DSS v2.0

Pritam Bankar, CISA, CISM, is a senior consultant within the Infrastructure Management Services group of Infosys Technologies Ltd. He has more than seven years of experience and has led several IT strategy consulting engagements in the areas of information security, IT/IS audits, compliance and regulations, and IT governance.

Sharad Verma is a consultant with Infosys Technologies Ltd. and has more than three years of diversified experience across various domains. He has worked in capability development for the Payment Card Industry Data Security Standard [PCI DSS] and has designed a (PCI DSS) framework for Infosys. He has expertise in the security domain and has experience in implementing ISO 27001.

On 28 October 2010, the PCI Security Standards Council released version 2.0 of the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., to help facilitate the broad adoption of consistent data security measures on a global basis. The standard provides controls and guidelines to secure cardholder data that are stored, processed or transmitted by merchants and other organizations.

This article is intended to showcase the changes made to PCI DSS v2.0 over v1.2 to further assist with detailed understanding of the control requirements to facilitate the PCI compliance process. Version 2.0 may bring more opportunities and flexibilities in PCI operations and cost reductions for organizations.

The revised standard provides additional guidance and minor clarifications. The changes fall mainly into three categories:

- **Clarification**—Modified wordings to portray the desired intent of the requirements
- **Additional guidance**—Added information to increase understanding of the intent of the original requirement, to assist in better implementation
- **Evolving requirements**—Added requirements to ensure that standards are up to date with emerging threats and changes in the market

Details of the differences from PCI DSS v1.2 to v2.0 are outlined in **figure 1**.

Figure 1—Differences Between PCI DSS V1.2 and V2.0

Requirement	PCI DSS V2.0	PCI DSS V1.2	Change Description
Scope	All locations and flows of cardholder data should be identified and documented. It clarifies that system components also include virtualization, i.e., virtual machines, virtual routers/ switches, applications.	No equivalent mention	In v2.0, the council made it clear that all locations that store, transmit or process cardholder data are in scope. The council also acknowledged the use of virtualization practice by explicitly mentioning it in the Scope section of PCI DSS v2.0.
1.3.5	Do not allow unauthorized outbound traffic from the cardholder data environment (CDE) to the Internet.	Restrict outbound traffic from the CDE to the Internet such that outbound traffic can access only IP addresses within the DMZ.	Under v1.2, merchants were not permitted to send encrypted information from the CDE environment to IP addresses outside the DMZ even with proper justification and business need. Under v2.0, a merchant can now bypass the DMZ and open outbound ports to transmit encrypted information from one trusted network to another—but only with a legitimate business reason and explicit authorization from the merchant.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Figure 1—Differences Between PCI DSS v1.2 and v2.0 *(cont.)*			
Requirement	**PCI DSS V2.0**	**PCI DSS V1.2**	**Change Description**
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from coexisting on the same server.	Implement only one primary function per server.	In v1.2, it was unclear whether one physical server could have two virtual components. In v2.0, the council clarifies that there can be two virtual functions on the same physical server running side by side. This will increase virtualization adoption by an organization and will help with cost savings.
3.2	Do not store sensitive authentication data after authorization (even if encrypted). Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data are stored securely.	Do not store sensitive authentication data after authorization (even if encrypted).	This is more of an exception for issuers and issuing service providers regarding the storage of authentication data. A qualified security assessor (QSA) is not expected to verify with issuers/issuing service providers that valid business justification exists for storing or retaining sensitive authentication data.
3.4	Where hashed and truncated versions of the same primary account number (PAN) are present in an entity's environment, ensure that additional controls are in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	No corresponding requirement	V2.0 explicitly mandates the masking of only PAN information. It enforces additional controls for security measures, as the original PAN can be reconstructed from hashed and truncated versions through trivial techniques. Additionally, if PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable.
3.6	3.6.4 Implement cryptographic key changes for keys that have reached the end of their crypto period. 3.6.5 Implement retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised. 3.6.6 If manual clear-text cryptographic key management operations are used, manage these operations using split knowledge and dual control.	3.6.4 Implement periodic cryptographic key changes at least annually. 3.6.5 Implement retirement or replacement of old or suspected compromised cryptographic keys. 3.6.6 Implement split knowledge, and establish dual control of cryptographic keys.	V2.0 increases flexibility in terms of the frequency of cryptographic key life-cycle changes (crypto period) based on industry best practices rather than, as per v1.2, changing it annually, which is a costly and time-consuming activity. V2.0 specifically provided reference to the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57. V2.0 reminds people to retire or replace keys whenever the integrity of keys is questioned. QSA will have to verify that such keys are not used for encryption. In v2.0, manual cryptographic key management operations must be managed by split knowledge and dual control of keys. To summarize, v2.0 suggests using the best practices from the industry standards and specifically refers to NIST SP 800-57.

Figure 1—Differences Between PCI DSS v1.2 and v2.0 *(cont.)*			
Requirement	**PCI DSS V2.0**	**PCI DSS V1.2**	**Change Description**
4.1.1	The use of WEP as a security control was prohibited as of 30 June 2010.	For new wireless implementations, it is prohibited to implement WEP after 21 March 2009. For current wireless implementations, it has been prohibited to use WEP since 30 June 2010.	V1.2 absolutely prohibited the use of WEP in the CDE after 30 June 2010; v2.0 clarifies that "WEP as a security control is prohibited," which means that one can still use WEP, but with an additional security/ encryption layer (e.g., SSL).
6.2	Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	Establish a process to identify newly discovered security vulnerabilities (e.g., subscribe to alert services that are freely available on the Internet).	V2.0 introduces the risk-ranking concept. It is recommended that merchants identify the vulnerabilities and rank them as high, medium and low, based on the risk to the organization and potential damages. This will help merchants focus on high-risk vulnerabilities and plan for remediation. The same is also applicable to 11.2.1 and 11.2.2; perform quarterly internal and external vulnerability scans where high vulnerabilities should be remediated to minimize the risk. Organizations can develop their own risk-ranking methodology based on their needs and size.
6.5	Develop applications based on secure-coding guidelines. Prevent common-coding vulnerabilities in software development processes.	Develop all web applications (internal and external, including web administrative access to the application) based on secure-coding guidelines such as the Open Web Application Security Project (OWASP) guidelines.	V2.0 does not restrict the use of coding techniques only to OWASP for developing secure applications. Organizations are given the flexibility to use any industry standard based on their needs. Also, the requirement now applies to all applications, not just web applications as noted in v1.2. The same is applicable to 11.3.2; perform penetration testing on all applications, not just web applications.
8.3	Incorporate two-factor authentication for remote access to the network by employees, administrators and third parties (e.g., remote authentication and dial in user service [RADIUS] with tokens, terminal access controller access control system [TACACS] with tokens, or other technologies that facilitate two-factor authentication).	Incorporate two-factor authentication for remote access to the network by employees, administrators and third parties. Use technologies such as RADIUS, TACACS with tokens, or virtual private networks (VPNs) (based on SSL/TLS or IPSEC) with individual certificates.	V2.0 further clarifies this requirement and explains the meaning of two-factor authentication; an additional authentication item must be used in conjunction with a password. There are three authentication techniques: 1. Something one knows (e.g., password) 2. Something one has (e.g., token, smart card) 3. Something one is (e.g., biometrics, retina, fingerprints) Per v2.0, organizations should use two of the three authentication techniques.

Figure 1—Differences Between PCI DSS v1.2 and v2.0 *(cont.)*			
Requirement	**PCI DSS V2.0**	**PCI DSS V1.2**	**Change Description**
11.1	Test for the presence of wireless access points, and detect unauthorized wireless access points on a quarterly basis.	Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	V2.0 provides more flexibility to merchants in terms of using any suitable method for detecting unauthorized wireless access points. Methods that can be used are wireless network scans, physical/logical inspection of system components and infrastructure, network access control (NAC), or wireless IDS and IPS.
11.4	Use IDS or IPS to monitor all traffic at the perimeter of the CDE and at critical points inside of the CDE, and alert personnel to suspected compromises.	Use IDS or IPS to monitor all traffic in the CDE and alert personnel to suspected compromises.	Merchants have flexibility in monitoring the traffic for any intrusion at the critical points inside the CDE rather than monitoring all the traffic by default. V2.0 recommends using IPS/IDS to monitor traffic at the perimeter and at critical points inside the CDE. This will save organizations time and money.
12.3	12.3.1 Obtain explicit approval by authorized parties. 12.3.4 Ensure the labeling of devices to determine owner, contact information and purpose. 12.3.9 Activate remote-access technologies for vendors and business partners. 12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copying, moving and storing cardholder data on local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	12.3.1 Obtain explicit management approval. 12.3.4 Ensure the labeling of devices with the owner, contact information and purpose. 12.3.9 Activate remote-access technologies for vendors. 12.3.10 When accessing cardholder data via remote-access technologies, prohibit copying, moving and storing cardholder data on local hard drives and removable electronic media.	In v2.0, this was modified to include approval from authorized parties rather than management. The same is applicable in 6.4.2 and 7.1.3, in which strong access controls are to be implemented after documented approval from authorized parties. In v2.0, the council makes it clear that the intention of this requirement is to determine the owner of the asset. In v2.0, remote-access activation applies to both vendors and business partners, not to vendors only. In v2.0, the requirement is updated to allow for controlled copying, moving and storing of cardholder data when accessing remotely—however only for legitimate reasons with explicit approval.
12.8	Maintain a program to monitor the service providers' PCI DSS-compliance status at least annually.	Maintain a program to monitor service providers' PCI DSS-compliance status.	This is more of a clarification regarding the frequency required for the PCI DSS-compliance status of service providers.

CONCLUSION

Even though there are no major changes, this version was much needed to provide the clarifications and justifications for the existing control requirements. IT and security teams will have to make best assumptions and judgment while implementing and complying with PCI controls.

Although it is encouraged to use v2.0 immediately, v1.2 will remain effective until 31 December 2011 to allow merchants to adopt any necessary changes in order to maintain their PCI DSS-compliance status. PCI DSS operates on a three-year life cycle, which means that it will take at least another three years for a new version to be released. Until then, organizations have time to focus on and implement the processes and controls to secure cardholder data and comply with PCI DSS v2.0.

REFERENCES

PCI Security Council web site, *https://www.pcisecuritystandards.org*

PCI Security Council, PCI DSS v2.0 and v 1.2, *https://www.pcisecuritystandards.org/security_standards/documents.php*

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.