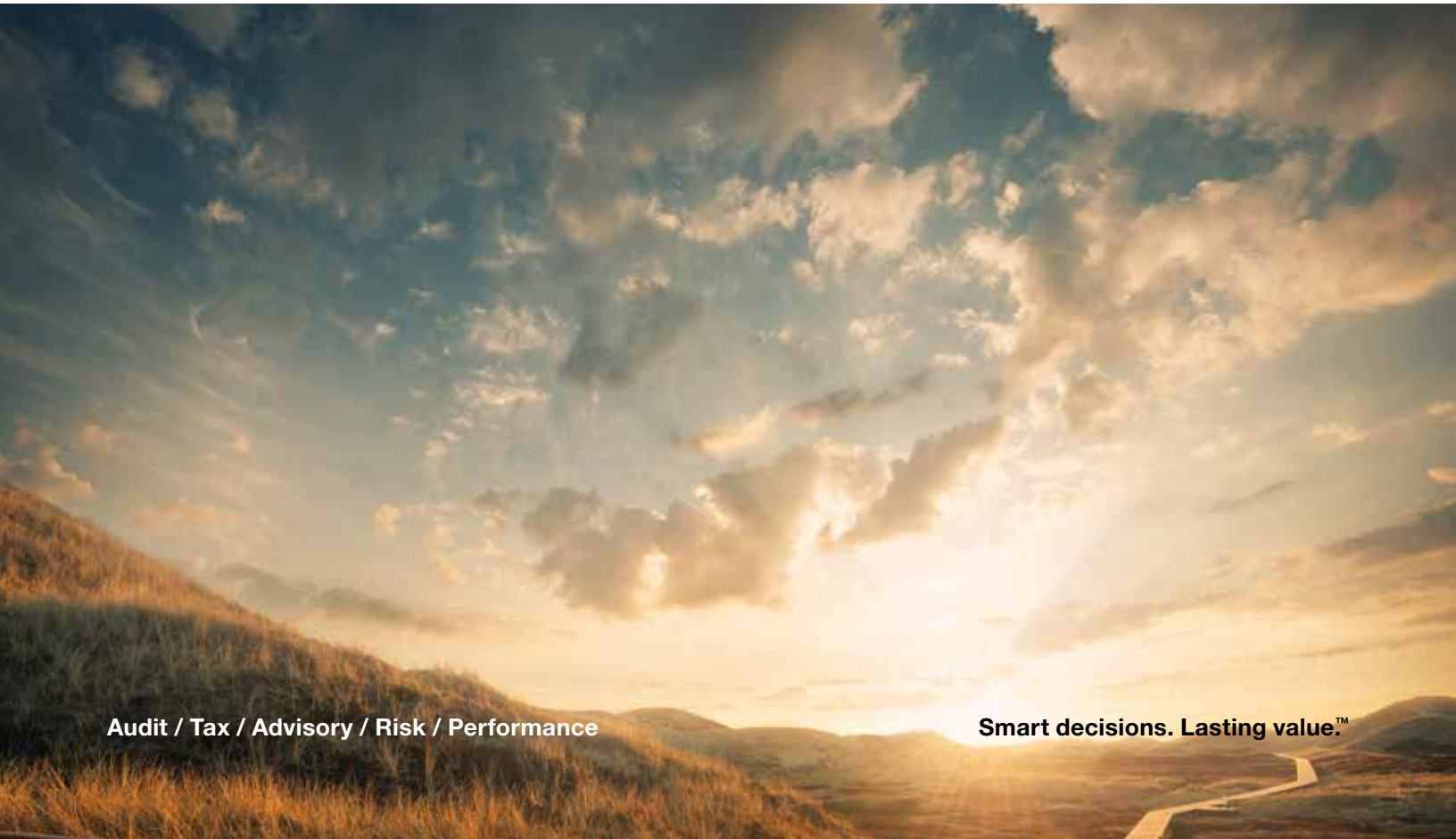
Crowe

April 2017

PCI DSS and Third-Party Risk Management

An article by Angela K. Hipsher-Williams, CISA, QSA; Sean F. McAloon, CISA, QSA; and Jonathan J. Sharpe, CISA, QSA



Data security standards for cardholder data are undergoing significant changes, with an emphasis on improving the security practices of third-party service providers.

The PCI Security Standards Council (SSC) has responded to recent data breaches involving third-party service providers by enhancing both its Data Security Standard (DSS) and the associated "Self-Assessment Questionnaire D and Attestation of Compliance for Service Providers." This response is not particularly surprising, given that 97 percent of breaches involving stolen credentials resulted from legitimate access by third-party service providers that aggregate significant amounts of credit and debit card information on behalf of their customers.[1]

PCI DSS version 3.2 was released in April 2016, and the previous standard (version 3.1) was retired at the end of October 2016. As of Nov. 1, 2016, all assessments must be performed according to the new standard. Most of the major changes in version 3.2 apply to service providers only, as companies that handle credit card data increase their scrutiny over providers due to providers' involvement in recent breaches. However, organizations also must take some critical steps to manage third-party risk and comply with the latest version.

Focus on Third-Party Service Providers

For payment card industry (PCI) purposes, a "third-party service provider" is defined as any vendor that stores, processes, or transmits cardholder data (CHD) on behalf of a client organization, as well as any vendor that could affect the security of the cardholder data environment (CDE). The latter is often overlooked.

While many organizations already have vendor management programs in place, they might also share CHD with several types of providers that are not necessarily included in those programs, such as:

- Infrastructure management companies
- Managed services companies
- Web hosting providers
- Backup tape storage facilities
- Transaction processors
- Payment gateways
- Fraud services

Organizations of all kinds have increased their use of third-party vendors. A Crowe survey found that 65 percent of respondents across industries make significant or extensive use of third-party vendors. Ninety-one percent indicated that technology vendors are significant to their business model, and 76 percent said that business services are significant to their model.[2]

As use of these vendors has ramped up, so, too, has the incidence of breaches originating with third parties rather than the breached entity itself. Of course, the breached entities suffered reputational damages and/or financial losses despite their lack of culpability.

Recent breaches at Home Depot, Target, and Lowe's were all widely covered in the media when they occurred. Additional noteworthy examples include:

- Banner Health (June 2016): Third-party owned and managed point-of-sale (POS) systems connected on Banner's network were compromised, exposing 3.7 million cards.
- Wendy's (May 2016): Third-party service provider POS remote access credentials were compromised at 1,025 locations.
- Jimmy John's (September 2015): Third-party service provider POS remote access credentials were compromised at 216 locations.

Many of the merchant breaches have targeted multiple points of weakness, including:

- Vendor-owned or -managed systems
- Vendor remote access to the CDE
- Information provided to third parties
- Information entered into third-party provider websites

PCI DSS Version 3.2 Compliance

The new version of PCI DSS reflects the heightened scrutiny of third-party service providers following the wave of breaches. It imposes several new responsibilities on providers. (Note that the new standard also includes changes that apply to all organizations, not just service providers.)

Following are a few important requirements of PCI DSS version 3.2 that organizations should adhere to. The list is not comprehensive and the items included are applicable mainly to service providers.

Requirement 3.5.1: Maintain documented description of cryptographic architecture.
Providers must understand all algorithms, protocols, and cryptographic keys protecting CHD. They also must keep inventory of all key management devices, including host security modules and secure cryptographic devices. These practices

might already be inherently occurring at a provider, but the explicit requirement for such activities pushes providers to verify that they are considering all relevant pieces.

Requirement 10.8: Detect and report failures of critical security control systems.
This requirement represents an attempt to reduce the period of time between discovering and reporting a breach. Providers must have formalized procedures for detection and documentation of the failure and documentation of the restoration of failed security functions.

Requirement 11.3.4.1: Perform penetration testing on segmentation controls at least every six months.
PCI DSS version 3.2 increases the frequency for required penetration testing from annually to semiannually. Additional testing is still required after any changes to segmentation controls.

Requirement 12.4.1: Establish responsibilities for the protection of cardholder data and a PCI DSS compliance program.
Protecting CHD and establishing compliance programs both were implicitly called for by version 3.1, but the new version explicitly requires providers to assign responsibility for the compliance program as a whole, as opposed to only for individual pieces.

Requirement 12.11: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures.
These reviews must take place quarterly instead of annually. Reviews must validate that existing policies and procedures are being followed with daily logs, firewall rules, configuration standards, security alert response, and change management. The idea is to confirm that the employees carrying out the different security-related tasks understand the related requirements and how they are to be satisfied.

Although PCI DSS 3.2 is not yet in full effect, all assessments dated on or after Nov. 1, 2016, must be performed according to the new standards. The new requirements will be best practices until Jan. 31, 2018, after which they will become mandates. The deadline for transport layer security (TLS) 1.2 migration has been extended to June 30, 2018, from June 30, 2016, but all new implementations going forward must be enabled with at least TLS 1.1.

Develop a Comprehensive Vendor Management Program

Requirement 12.8 of PCI DSS version 3.2 requires all organizations to maintain and implement policies and procedures to manage service providers with whom CHD

is shared, or that could affect the security of cardholder data. In other words, when sharing CHD with service providers through different means, an organization must have a comprehensive program to ensure that those providers will protect the data. The program should incorporate several components.

Three Pillars of Effective Vendor Management

Effective vendor management programs are built on three pillars: due diligence, ongoing management, and periodic evaluation.

1. **Due diligence**. Organizations must establish a process, including proper due diligence, for engaging service providers prior to engagement. They should assess the risks presented due to a new, renewing, or expanded relationship, bearing in mind the services to be provided, and determine current and planned controls to manage the risks. To do so, an organization should perform an inherent risk assessment, followed by a ranking of the risks. This will allow a risk-based approval or rejection of contracts by senior management. In addition, the contractual assignment of PCI DSS responsibility between the entities should be reviewed to confirm that the applicable requirements are met, and compliance should be validated.
2. **Ongoing management**. Organizations are required to maintain a program to monitor service providers' PCI DSS compliance status at least annually. They also should manage the day-to-day relationship and performance of the provider by confirming that management and control activities are performed and any issues or incidents are addressed in a timely fashion. Ongoing management further includes communications and stakeholder management. Organizations also should know the compliance status of their service providers and obtain providers' attestations of compliance.

   Some organizations might find it useful to go beyond the annual review requirement and monitor more frequently or with additional procedures. For example, an organization might also evaluate a provider's business strategy (including any acquisitions or divestitures), insurance coverage, or ability to respond and recover from certain service disruptions.
3. **Periodic evaluation**. The PCI DSS requires organizations to specify which PCI DSS requirements are managed by each service provider and which are managed by the organization. They must periodically re-evaluate the risk of the relationship based on a risk assessment, as well as when incidents or performance issues arise (for example, a breach or service disruption or the expiration or termination of a contract). In some cases, organizations might have to adjust or implement controls and modify ongoing management.

Know Your Third Party

Organizations also should adopt a "know your third party" framework, based on governance and management principles, to support the process of third-party risk management.

The governance principles suggest organizations take the following steps:

1. **Identify**. The organization should know who it does business with and how its providers can affect the PCI environment. Common gaps include the lack of a consistent onboarding process for new vendors, failure to identify all vendors with whom data is shared, and assumptions that money spent on a particular vendor is an indication of that vendor's risk. In reality, risk is affected much more by how a vendor shares information with other vendors.
2. **Assess**. The organization must understand the risks of the identified relationships.
3. **Manage**. The organization must take action to address the third-party risks by developing an approach based on the risks of each vendor. Addressing risks should take place on an ongoing basis after onboarding has occurred.
4. **Control**. The organization should manage and control the third-party risk management program and assign responsibilities to appropriate stakeholders.

The management principles encompass standards, procedures, and technology. Standards are the meat of the program (and therefore are rarely changed), highlighting the need for a holistic program. Procedures are the working processes that are followed for vendors; they provide the detail on the actual execution of the plan outlined in the standards. Both standards and procedures should be included in documentation governing the program and its expectations. On the technology side, organizations must establish systems that support efficient and effective execution of their third-party risk management programs.

Action Items

In response to the new PCI DSS requirements, individuals charged with PCI compliance and vendor management will need to:

- Include PCI-related vendors in the overall vendor management program and verify that appropriate attention is paid to all vendors that are storing, processing, or transmitting CHD on behalf of the organization
- Develop a classification system for vendors that can affect the security of the CDE
- Assign qualified individuals to review, interpret, and determine reliance in cases in which the program is receiving attestations
- Present PCI-related vendors to the audit committee with information explaining any associated risks

Act Now

Although the new requirements are not yet in effect formally, organizations need to take prompt action to position themselves and their third-party service providers for compliance when the time comes. They must understand the numerous changes associated with PCI DSS version 3.2 and begin to build a comprehensive third-party risk management program that will meet the intent and rigor of the requirements and effectively manage their risk.

Learn More

Angie Hipsher-Williams
Principal
+1 317 208 2430
angie.hipsher@crowe.com

Sean McAloon
+1 214 777 5228
sean.mcaloon@crowe.com

Jonathan Sharpe
+1 317 208 2433
jonathan.sharpe@crowe.com

---

[1] Verizon 2016 Data Breach Investigations Report, p. 33, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[2] Rick Warren, "Closing the Gaps in Third-Party Risk Management: Defining a Larger Role for Internal Audit," sponsored by the Institute of Internal Auditors Research Foundation and Crowe, 2013, p. 10, http://cdn.cfo.com/content/uploads/2013/12/Crow_IAA_Study.pdf

crowe.com

Text created in and current as of April 2017; Cover and artwork updated in May 2018.

RISK-17012-005A