globalscape™
securely connected

Whitepaper

Protecting Payment Information with PCI DSS Version 3 Compliance

Introduction to PCI DSS Version 3

When a string of large-scale, high-profile retail data breaches hit last year, credit card data security stole the national spotlight and remains prominent in the minds of many consumers and industry leaders now. How can businesses better fortify their systems against the malicious activity of hackers, as well as guard against accidental mishaps that expose sensitive information? As with any security effort in this increasingly complex digital environment, it's an ongoing dialogue, and one that requires constant vigilance and revisiting.

The Payment Card Industry's Data Security Standard (PCI DSS) is a set of guidelines for electronic payment processing. Overseen by a council formed by the four major credit card providers in 2006, PCI DSS provides guidelines to ensure a secure environment for transaction information, ultimately guarding against fraud and identity theft.

The PCI's Security Standards Council maintains the PCI DSS, revising the protocols regularly to adapt to an evolving technological landscape. In November 2013, the council issued version 3 of its standards. PCI DSS version 3 took effect on January 1, 2014, but existing PCI DSS version 2 vendors will have until 2015 to move to the new standard.

In general, the revisions encourage organizations to make PCI DSS compliance an ongoing state, rather than a milestone to achieve at the moment of auditing. By emphasizing education and more robust best practices that recognize evolving technology trends, the updated standards call for greater cooperation between enterprises and deeper oversight of tech practices.

Complying with the regulations won't guarantee that a company is safe from a data breach, but it's an excellent step toward better protection.

Who Needs to Abide?

The PCI DSS is not a law, which means that businesses are not legally obligated to comply with the standards. However, the four major credit card companies (American Express, Discover, MasterCard, and VISA International) and JCB International Credit Card Company require organizations to comply with these measures in order to process credit card payments.

The PCI DSS is one of the most widely accepted set of standards for protecting payment information. It's globally recognized and offers an "actionable framework for developing a robust payment card data security process," according to the PCI website. Establishing a network based on these recommendations is a solid foundation for protecting cardholder data at rest and in transit.

Organizations that comply with the PCI DSS enjoy the following benefits:

> Keep their systems secure, preventing costly data breaches
> Build trust with business partners, other merchants, and customers
> Improve their reputation within the industry

In addition to avoiding fines and legal actions, enterprises should implement PCI DSS as one way to reduce the chances of a data breach occurring in the first place. According to the Ponemon Institute's "2014 Cost of Data Breach: Global Analysis" report, data breaches cost companies an average of $3.5 million in 2014 when all of the expenses involved in responding to an incident were considered, representing a 15 percent increase over the previous year.

What do the Standards Cover?

Merchants can review the complete standards on the PCI website at https://www.pcisecuritystandards.org/security_standards/documents.php. In general, the recommendations cover the prevention, detection, and appropriate response to security incidents, while creating a framework for organizations to design less vulnerable systems to prevent data breaches from occurring in the first place.

The changes incorporated into version 3 of the PCI DSS controls focus on four key areas that the council recognized as in need of improvement:

> Education and awareness to ensure employees are partners in upholding security
> Increased flexibility for ways that organizations can meet standards, particularly in terms of passwords and authentication
> Security as a shared responsibility, encouraging companies to work with their business partners to uphold best practices and requirements
> Emerging technologies, especially e-commerce, mobile, and cloud computing platforms

In general, these changes point to the need for more intuitive, integrated approaches that can be actively and consistently upheld by all players through every point of the transaction process. While some of the new protocols address common-sense issues, such as password best practices, others may require IT teams to take a closer look at their IT infrastructure, physical security, data management, and coding practices.

Additionally, there are now standards for working with service providers to ensure all aspects of the system, even those in the cloud, are compliant. These changes come as a response to a growing dependency on managed and Software-as-a-Service offerings, particularly as enterprises increasingly adopt the cloud.

McGladrey Consulting Services identified some of the most significant changes in terms of their impact on businesses. Some of these, such as requirement 6.5.6, have to do with the way in-house developed apps are coded and protected by encryption. Others, including requirement 12.4.1, dictate how system architecture should be designed, with some components kept separate from others. Thus, home-grown and fragmented systems will be more complicated to manage, which means that a comprehensive, unified solution can ease some of the burden of PCI DSS version 3 compliance.

Companies also need to increase their documentation to demonstrate compliance, train personnel on the guidelines, and perform more extensive penetration testing to ensure their systems are consistent with the standard.

Why Choose Globalscape?

Complying with the PCI DSS, like other security approaches, is never a "set it and forget it" step—particularly with the changes made in version 3 to emphasize ongoing vigilance. Viewing compliance as a matter of completing a checklist and receiving certification is neither effective nor helpful. In fact, in the event of a breach, organizations must not only be registered as compliant but actively in compliance at the time of the incident to avoid fines and fees. Furthermore, only by implementing the standards in a comprehensive, integrated manner can businesses have confidence that the measures will help to protect their systems.

Managed file transfer solutions offer organizations a streamlined approach to implementing the correct encryption and data management protocols to comply with recommendations. However, MFT alone still leaves IT teams with a lot of work to do to meet remaining requirements—such as the need for a demilitarized zone. Instead of integrating these components on their own, businesses can turn to more comprehensive solutions that offer more robust features that enable them to meet PCI DSS compliance. This approach helps to close the gaps while providing a system that's easier to manage and adapt to updated requirements.

As a best-in-class, global leader in the secure file transfer industry, Globalscape makes PCI DSS compliance a top priority within its highly secure Enhanced File Transfer™ (EFT™) solutions, which go a step above and beyond other MFT offerings. Not only is Globalscape's EFT solution already compliant with version 3, it offers both the technology and the expertise to help companies establish a robust, secure system in line with PCI DSS requirements. This makes it easier for organizations to establish, maintain, and report on systems in a compliant manner.

Many organizations struggle to implement PCI DSS effectively and demonstrate that they're compliant. For example, a recent study by network security provider Fortinet revealed that 20 percent of small and medium business retailers lack fundamental security and fail to comply with the PCI DSS. Even organizations that achieve compliance have difficulties maintaining it consistently year-round. That's why it's important for companies to choose solutions that can verify their compliance and offer integrated systems and vendors that can offer the level of support necessary for administrators to quickly and easily put compliant systems in place

Globalscape's Tools for Compliance

At a broad level, Globalscape assists organizations by offering managed file transfer, Mail Express®, and mobile clients that are integrated into a single, secure platform in a compliant manner. These products facilitate dependable, compliant data transfer and storage. Businesses can implement these solutions in PCI DSS mode using convenient, intuitive setup wizards and count on the added protection of the High Security Module (HSM), which is available for the MFT product.

Globalscape solutions are designed to protect sensitive information both at rest and in transit. Data is managed and controlled through a central, secure point. Furthermore, Globalscape's cryptographic module is FIPS 140-2-validated for SSH and SSL connections and EFT completely sanitizes deleted data per PCI DSS requirement 9.8.

For information in transit, the HSM offers the following benefits:

- Stores and disposes of data securely
- Requires passwords and account access policies that comply with standards
- Uses only strong encryption ciphers and keys
- Reports violations and applies compensating controls
- Monitors and logs user activity
- Identifies, assesses, and alerts administrators when non-compliant events occur
- Generates reports for auditing

Additionally, Globalscape's demilitarized zone proxy network, DMZ Gateway®, establishes multi-layered security without storing data. This complies with PCI DSS requirements without sacrificing efficiency or performance. The optional DMZ Gateway enables companies to meet specific standards that are not supported by less robust MFT offerings, including requirement 1.3, which prohibits direct public access between the Internet and any system component in the cardholder data environment.

Globalscape's products use a wide range of secure user authentication sources, including Active Directory, NTLM, LDAP, and ODBC-compatible databases, so EFT solutions can be fully integrated with customers' existing infrastructure.

Ongoing, active compliance is supported through the Auditing and Reporting Module (ARM), which offers daily compliance reports—which is particularly important in light of the new, more comprehensive documentation requirements. With daily reports, businesses can be confident that their system meets the rigorous compliance standards throughout the year, not just when it's time for their annual PCI audit. If problems do arise, the reports include explanations of compensating controls (workarounds), which administrators can put in place to bridge the gaps.

Although Globalscape's EFT facilitates PCI DSS compliance and can help organizations implement systems that uphold PCI requirements, the DSS controls include some measures that must be addressed in technology solutions outside of EFT. Business leaders are ultimately responsible for ensuring that their systems cover all of the requirements, including educating employees and conducting the appropriate penetration tests.

Conclusion

PCI DSS compliance is an important step toward protecting sensitive payment information and building relationships of trust with customers and partners. The need for secure systems that guard credit card information has never been more pressing: With data breaches on the rise and cybercriminals developing increasingly sophisticated approaches, organizations are under pressure to harden their infrastructures. While no strategy has shown to be completely effective, the PCI DSS serves as a strong foundation for a comprehensive data security approach.

Business leaders and IT teams are under increasing pressure. As version 3 of the DSS addressed, omnichannel research introduces greater complexity into electronic transaction systems, incorporating multiple platforms, various devices, and growing volumes of data. Therefore, establishing a PCI-compliant system can be difficult to implement, monitor, and maintain. With Globalscape's reliable tools, expert support, and robust reporting resources, companies can get off to a strong start and demonstrate their commitment to information security.

Sources

https://www.pcisecuritystandards.org/security_standards/index.php
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
https://www.pcicomplianceguide.org/pci-faqs-2/
http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard
https://financial.ucsc.edu/Pages/Security_Penalties.aspx
http://www.cardfellow.com/blog/pci-non-compliance-fee/
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf
http://investor.fortinet.com/releasedetail.cfm?releaseid=818870
http://www.globalscape.com/mft/pci.aspx
http://www.globalscape.com/mft/dmz-gateway.aspx
http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
http://mcgladrey.com/content/dam/mcgladrey/pdf_download/pci-guidelines.pdf

About Globalscape

Globalscape ensures the reliability of mission-critical operations by securing sensitive data and intellectual property. Globalscape's suite of solutions features Enhanced File Transfer™, the industry-leading enterprise file transfer platform that delivers military-grade security and a customizable solution for achieving best-in-class control and visibility of data in motion or at rest, across multiple locations. Founded in 1996, Globalscape is a leading enterprise solution provider of secure information exchange software and services to thousands of customers, including global enterprises, governments, and small businesses.