IBM Commerce
Whitepaper

Profiting from PCI compliance

Why investing in PCI compliance means a better bottom line.

IBM

Contents

Executive Summary

Working together back in 2004, the major payment card providers developed a set of data security standards and created a council for enforcing them. Although today the Payment Card Industry Data Security Standard (PCI DSS) has become a global requirement, many organizations are still lagging in compliance or struggling to maintain compliance when new mandates are released. For many companies, regulatory compliance can already be an overwhelming, costly and confusing area to navigate, and the need to comply with the PCI DSS might feel like yet another burden. However, IBM believes that the PCI standard should instead be seen as an opportunity for your organization. The standard is so well designed now that it can actually serve as the foundation of your risk management strategy going forward. This document explores the efficiency gains of building a strategy designed around PCI compliance. As it discusses the value of obtaining outside support in your compliance efforts, it also examines potential vendor qualifications.

Rethinking PCI requirements.

A number of high-profile security breaches and identity theft operations have driven several companies out of business or caused extensive financial and brand-related damage and have highlighted the need for security protocols that protect consumer payment data. In 2014, during one of the largest payment card breach to date, Adobe experienced approximately 150 million stolen customer records. In 2007 TJ Maxx breach compromised over 90 million customer records. Smaller breaches, though less likely to generate headlines, have nevertheless threatened to undermine consumer confidence and put businesses that accept card payments at risk.

The standard itself was created as a joint effort by Visa International and MasterCard Worldwide. Then, in September 2006, these two payment card providers joined American Express, Discover Financial Services and JCB to form the PCI Security Standards Council and extend the standard globally across the card brands.

An IBM global study in 2015 showed that malicious or criminal intent accounted for 47% of all cyber breach attacks[1].

While the PCI standard might seem like another snarl of red tape to companies already burdened with financial services industry regulations such as International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002 and the Sarbanes-Oxley Act, the standard can actually simplify your job enormously. It is so comprehensive and well designed that it can be seen as a compliance enabler for a broad set of industry regulations. And because privacy is a core concern for almost all businesses, PCI standard compliance supports your bottom line.In fact, the PCI standard can actually become the central principle around which your overall governance and risk management strategy can be organized. By adopting the PCI standard as a best practice and aligning its security measures with your business processes, you will likely see significant gains in efficiency and data security. A review of the sidebar on this page illustrates that the practices that comprise the PCI standard are best practices for any security strategy, period.

Mapping PCI compliance to overall financial governance and payments management strategy

There is no need to approach PCI compliance as a separate issue for your business. Governance and risk management, also known as enterprise risk management, supplies the philosophical basis for the PCI standard. Way back in 2004, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission released an integrated framework for

1 IBM 2015 Cost of Data Breach Study

"Retailers themselves are coming to the conclusion that they need some better protocols and standards. At the very least, they need some real-time information sharing."

—Tim Pawlenty
CEO of the Financial Services Roundtable

enterprise risk management to provide guidance and benchmarks designed to enable organizations to:

- *Align their risk tolerance with strategic business goals.*
- *Measure risk and determine how taking risks affects growth.*
- *Create greater flexibility in risk mitigation and incident response.*
- *Identify and correlate cross-enterprise risks.*
- *Develop a cross-enterprise governanace and risk managment capability.*
- *Respond to business opportunities with an understanding of the full range of events within the organization*
- *Make better capital investments by more effectively assessing risk.*

The PCI standard was designed to encompass the four critical areas of the COSO framework, as follows:

- *Event identification recognizes both the increased opportunity for sales through online retailing and the associated cardholder privacy issues.*
- *Risk assessment requires companies to realistically analyze the risks to their businesses, to customer privacy and card vendor.*
- *Risk response helps reduce the costs of managing risk by supplying a single set of security standards that enables organizations to comply with multiple card issuer agreements.*
- *Control activities establish clear guidelines and policies that everyone must follow, helping to boost consumer confidence and reduce the risk of non-compliance.*

"In the US malicious attacks cost an organization $230 per capita affected."

— IBM 2015 Cost of Data Breach Study

Fortunately, the processes of event identification, risk assessment, risk response and control activities are also relevant for compliance with a multitude of regulatory requirements, including the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA) and others. By adopting a governance risk management discipline that includes PCI alignment, an organization can streamline compliance activities, reduce duplicative efforts and decrease costs.

Understanding the challenges of becoming compliant

While PCI standards are simply worded and provide a good foundation for your governance and risk management strategy, you should be aware of a number of factors that can complicate the road to compliance.

For example, each payment card company, while adhering to a core set of standards, has its own particularities in terms of its exact enforcement mechanisms. These factors must be taken into account as you design your strategy.

To be prepared for the compliance assessment, you must have a certain number of checkpoints in place. You must also be able to demonstrate that you are not keeping data that the PCI standard specifies you are not entitled to keep. For example, full-track data from the magnetic card strip, PIN information or the card validation number (CVC, CVV2, CID) must never be retained.

The requirement to remove data that should not be retained also means wiping inappropriate data from all areas of the data stream. In the United States, using a U.S. Department of Defense–approved wiping process satisfies this requirement; while in other portions of the world, either the U.S. or European Privacy Act wiping process is required. These data stream areas include databases, backup files, transaction logs, application logs, device logs, error logs and reports, network sniffers, and core and memory dumps used for diagnostic purposes.

Recognizing the value of outside assistance and solutions in achieving PCI compliance

While some companies do elect to develop, deploy, assess and penetration test a compliance strategy on their own, others find that there are certain advantages to using a third-party vendor for these activities. For some organizations, an outside vendor can provide external validation that the appropriate processes and policies are in place; this validation can provide reassurance to customers, partners, shareholders and card issuers. A third-party vendor can also provide a fully compliant and certified payments acceptance hub with tokenization support that, once integrated, immediately brings your digital commerce solution into compliance and can significantly reduce time to market and overall cost.

When compliance validation activities and payment systems are executed in-house, company officials become fully liable for any omissions or errors. Using a third-party vendor can shift the risk away from corporate management. Companies can conduct their own penetration testing if they prefer. Quarterly external network scans are required for all merchants and service providers, and these scans must be performed by an approved third-party assessor. When companies reach a certain threshold of payment card transactions, a certified PCI assessor must be used to validate PCI compliance. The PCI Security Standards Council manages a Qualified Security Assessor (QSA) program, ensuring that assessors are fully certified to conduct PCI assessments.

Getting help

First you need to determine what level of PCI compliance planning you need. Do you need to simply upgrade your existing PCI payment acceptance solution to the new mandates or do you instead need a thorough investigation and compliance analysis as well of your overall business processes and systems? Turning over your customer payment data responsibility or allowing a third-party assessor to sift through your data can be a scary proposition, so it's important to choose a trusted, experienced, certified provider that understands the PCI standard in relation to your industry. The ability to handle all phases of your PCI compliance validation, from pre-assessment through report of compliance (ROC) submission, to delivery of a turn-key compliant payment acceptance solutions, is key.

As you proceed through the selection process, you should ask yourself these questions:

- *Is my vendor a trusted brand, do they have a history of expertise and high quality results when it comes to data security and cyber security analysis experiences?*
- *Does my vendor offer a turn-key PCI compliant payment acceptance solution that is easy to integrate with and reduces my burden of cost and resources?*
- *If I'm needing a full assesement, do I receive simply the output of an analysis or do I benefit from the vendor's security expertise.*

In short, you want a trusted security partner that can be your advocate and facilitator to your credit and payment partners.

Why IBM?

IBM Payments Gateway is a fully PCI v3.1 compliant solution in the cloud with tokenized transactions to eliminate the need for any merchant to maintain credit data within their corporate systems. With multiple integration methods for the web and mobile and hundreds of payment types and localized support around the globe, IBM Payments Gateway is a key component in the PCI strategy of any merchant.

IBM Security Services (ISS) is recognized by the Payment Card Industry as an approved provider of security assessment services for compliance with the PCI standard. ISS is 1 of 7 companies recognized globally as a Qualified Incident Response Company (QIRC).

To learn more about PCI compliant payment acceptance solutions and how IBM can help, please contact your IBM representative or visit: ibm.com/commerce or ibm.com/services/security.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January, 2016

Please Recycle