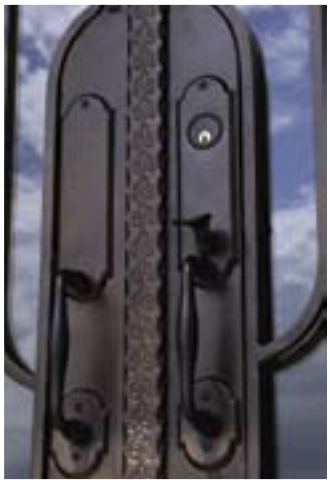
September 2007

Profiting from PCI compliance.








Contents

Executive summary

Working together, the major payment card providers have developed a set of data security standards and created a council for enforcing them. Although the Payment Card Industry Data Security Standard (PCI DSS) has become a global requirement, many organizations are lagging in compliance. For many companies, regulatory compliance can already be an overwhelming 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 that it can actually serve as the foundation of your risk management strategy going forward. This paper 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 and highlighted the need for security protocols that protect card data. In the largest payment card breach to date, TJX experienced approximately 45 million stolen 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.

The six categories of PCI best practices

Taken together, the six areas of data protection prescribed by the PCI standard help you build a comprehensive approach to overall security. They address security concerns from network protection to security governance policies.

- *Build and maintain a secure network.*
  - *Create a firewall to secure cardholder data.*
  - *Go beyond vendor defaults for passwords and other security parameters.*
- *Protect cardholder data.*
  - *Protect stored data.*
  - *Encrypt data transmission.*
- *Maintain a vulnerability management program.*
  - *Employ and update anti-virus software.*
  - *Develop and maintain application security.*
- *Implement strong access control measures.*
  - *Restrict access to cardholder data on a need-to-know basis.*
  - *Assign a unique ID to each authorized user.*
  - *Restrict physical access to cardholder data.*
- *Regularly monitor and test networks.*
  - *Track and monitor access to network resources and data.*
  - *Regularly test security systems and processes.*
- *Maintain an information security policy.*
  - *Develop and maintain policy-based security protocols.*

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.

Who must comply with the PCI Data Security Standard?

All merchants and service providers that store, process, use or transmit payment cardholder data must comply with the standard. The standard is enforced by the card companies and their acquirer banks.

Mapping PCI compliance to your overall governance and risk 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. In 2004, the Committee

Highlights

The COSO framework was designed to help organizations develop effective enterprise risk management strategies.

of Sponsoring Organizations (COSO) of the Treadway Commission released an integrated framework for 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 governance and risk management 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 to the 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 noncompliance.*

The PCI standard helps you prepare for compliance with a number of regulations.

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)

Highlights

and others. By adopting a governance risk management discipline that includes PCI alignment, your organization can streamline compliance activities, reduce duplicative efforts and decrease costs.

Understanding the challenges of becoming compliant

Beware of obstacles on the road to PCI compliance.

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 requirements and enforcement mechanisms. These factors must be taken into account as you design your strategy.

You must have certain checkpoints in place, and you must be able to demonstrate your compliance.

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 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.

Avoiding common errors

It can be helpful to know that certain errors are routinely identified in compliance assessments, including the following:

- *Storage of prohibited cardholder data*
- *Use of production cardholder data in test environments*
- *Failure to encrypt the full payment card number*
- *Lack of a network segmentation system that isolates the transaction environment*
- *Lack of segregation of internal staff duties*
- *Failure to label cardholder media as confidential*

Recognizing the value of outside assistance 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 an objective analysis of your current compliance status, along with recommendations for closing any gaps. (Because third-party assessors are required to provide at least three alternatives for technology and services vendors, you are protected against an independent vendor simply recommending its own solutions.)

When compliance validation activities 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 the majority of 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.

Selecting a third-party vendor

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

Proprietary tools and technologies from IBM

- *Consul InSight suite: collects and centralizes security log data, filters it against security policy, automatically triggers appropriate responses and alerts, archives log data and provides a dashboard for consolidated viewing and reporting*
- *IBM Internet Security Systems™ solutions: provide a protection platform that automatically guards against both established and unknown Internet-based threats and is driven by the advanced analytics developed by the IBM Internet Security Systems X-Force® security research and development team*
- *Additional IBM hardware, software and services (including IBM Tivoli® software, IBM System z™ encryption solutions and the IBM Resource Access Control Facility [RACF®] program): help optimize security, compliance, and the alignment of business and IT*

through report of compliance (ROC) submission, is key. Your vendor should be willing to offer you multiple alternatives for achieving the same level of protection and should provide you with a detailed roadmap in each case. The assessor's core competency should extend beyond compliance services to addressing your overall security posture and providing recommendations for securing your infrastructure. The services provided should be clearly delineated, particularly if the contract spans multiple years.

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

- *What am I getting for my investment? Do I receive simply the output of a scan, or do I benefit from the vendor's security expertise?*
- *How customized is the assessment that this vendor offers me?*
- *Is my vendor fully certified to perform all phases of the PCI compliance validation?*
- *Has this vendor fully explained the timeline involved in the process? From pre-assessment through ROC submission, the process can take from 9 to 18 months; am I prepared for that?*

In short, you want a trusted security adviser that can be your advocate to your acquirer bank and payment card companies.

Why IBM?

IBM Internet Security Systems (ISS) is recognized by the Payment Card Industry as an approved provider of security assessment services for compliance with the PCI standard. As a QSA, an Approved Scanning Vendor (ASV), and a Payment Application Best Practices (PABP) assessor, IBM ISS can help organizations comply with the PCI DSS. IBM ISS is also recognized as a Qualified Incident Response Company (QIRC).

IBM maintains a staff of highly skilled security professionals who have industry-specific expertise and use consulting methods based on ISO/IEC 27002 best practices. These abilities help us go beyond simply assessing your PCI compliance status to providing detailed recommendations for creating a comprehensive security strategy.

What's more, IBM's proprietary technologies and tools help you build a strategy to maintain compliance. We take pride in being a trustworthy resource with a strong track record to confidentially handle your sensitive data.

For more information

To learn more about PCI compliance and how IBM can help, please contact your IBM representative or IBM Business Partner, or visit:

ibm.com/services/security

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America
09-07

GTW01773-USEN-00