Meeting the 12 requirements for PCI-DSS compliance

IBM z Systems mainframes and IBM software solutions can help protect customer data and reduce payment card-related risk

IBM

Introduction

If you handle money using payment cards—whether as a retail store, restaurant, airline, bank, hospital or any of a wide range of sales and service organizations—you're subject to the Payment Card Industry Data Security Standard (PCI-DSS). This global security program was created in 2001 to increase confidence in the payment card industry and reduce risks to industry members, merchants, service providers and consumers.

PCI-DSS is not a law—but it is not simply a set of recommendations, either. It is an industry-backed program, run by the PCI Security Standards Council of card companies including Visa, MasterCard, American Express and Discover. Updated over the years to keep up with changing technology and evolving security threats, it establishes specific requirements an organization must meet in order to comply with protection standards. Significantly, it also establishes specific consequences for noncompliance.

In a world where threats to financial data are ever changing—and where attacks often come without warning out of the shadowy world of cybercrime—the structured PCI-DSS program is a specific, quantifiable and tangible mechanism for helping protect organizations and their customers from payment card-related risk.

This white paper examines the state of PCI-DSS compliance today, the quantifiable consequences— both from a security breach and from industry sanctions—that can follow noncompliance, and the specific steps organizations must take to be compliant. It examines the advantages of the mainframe as a platform that is especially well suited for ensuring compliance. It describes security software and systems management solutions an organization can deploy to help make compliance possible.

The state of PCI-DSS compliance today

Consider the scope and effects of cyber attacks. First, the sheer number of attacks is not only up, it is huge. In 2014 alone, across organizations of all kinds, there were nearly 43 million security incidents. This represents a compound annual growth rate of 66 percent since 2009.[1] For companies in the financial and retail industries, where cyber attackers clearly can profit from their actions, the consequences are also huge. An attack on JPMorgan Chase in 2014 compromised the accounts of 76 million households and seven million small businesses. The previous year, an attack on Home Depot affected 50 million cardholders, while an attack on Target affected 40 million cardholders.[2] Meanwhile, in Korea, a country of 50 million people, an attack captured personal data on nearly half its citizens, some 20 million bank and credit card users.[3]

It is precisely this type of "mass loss" or leakage of credit card information that PCI-DSS was created to prevent. PCI-DSS requirements address common security vulnerabilities in enterprise environments. And by meeting requirements, companies put into place measures that can help prevent the loss of valuable data. Standards allow self-certification for small businesses, but large organizations must be formally assessed by Qualified Security Assessors (QSAs) or Internal Security Assessors (ISAs)—a process that itself can help an organization identify and remedy gaps or weaknesses in systems where cardholder data is stored or transmitted.

Compliance alone, of course, does not guarantee complete safety, just as noncompliance does not guarantee an attack will succeed. The same can be said for security; it does not guarantee compliance. But for many companies, compliance with the PCI-DSS requirements does appear to help. One recent study of breached and un-breached companies found that the un-breached outperformed the breached by 36 percent in their PCI-DSS compliance.[1]

The benefits of complying with PCI-DSS

Cybercriminals are clever. In the case of JPMorgan Chase, hackers obtained a list of the bank's applications, which they cross-checked with known vulnerabilities to find access paths into computer systems.[2] So defenders need to be vigilant. In response, PCI-DSS sets up three steps to help: an assessment that inventories IT assets and business processes and then analyzes them for vulnerabilities, remediation of any vulnerabilities the assessment uncovers, and reporting to the PCI-DSS organization on remediation as well as requirement compliance. It is an ongoing process.

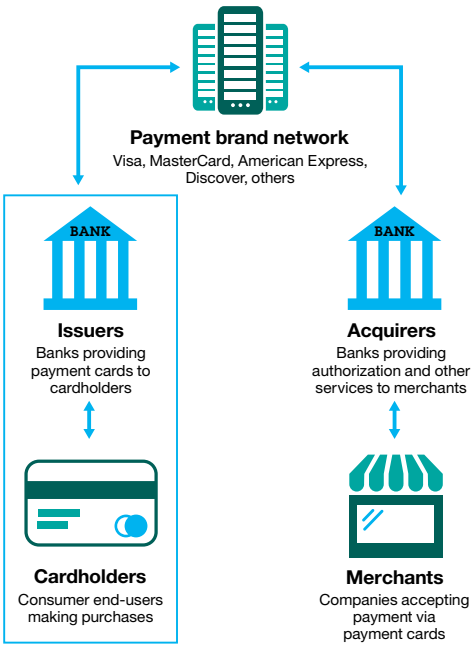
In support of security, PCI-DSS requirements are designed to help protect cardholder data for user authentication including the primary account number (PAN), cardholder name, expiration data and service codes. The ultimate goal is to benefit everyone in the purchase process with reduced risk, controlled liabilities and increased confidence in the payment card industry.

Consumers can gain peace of mind that their personal and financial information is protected and that they are less likely to be the target of identity theft. Merchants and service providers can increase revenues and gain a competitive edge by maintaining a positive image, protecting consumers and avoiding fines.

For merchants, service providers and financial institutions, there are natural benefits from avoiding the financial consequences of a breach—and according to one recent study, these are among the industries that suffer the greatest breach-related expenses. While the average cross-industry cost of a data breach for a single lost or stolen record was USD154, financial institutions incur an average cost of USD215. Retail organizations incur an average of USD165. But losses are growing faster in retail than in any other sector, up 57 percent from USD105 in a single year.[4]

A breached organization typically incurs IT staff costs for instating compliance measures, costs of notifying customers, the cost of possibly replacing payment cards, and reduced sales due to potential store closings or damage to consumer confidence. But the business cost of the breach is not the only consequence of noncompliance. If a security breach occurs, the PCI Security Standards Council can fine a noncompliant company up to USD500,000 per incident. Audit requirements can increase and credit card activity can be shut down.[5] With these consequences in mind, any business would do well to consider how long it could survive if its online systems or call centers were no longer allowed to accept payment cards to pay for goods or services.

Participants in managing payment card data



Low rates of achieving and sustaining compliance

Does the carrot-and-stick approach that on the one hand helps avoid the cost of a breach but on the other hand also carries the potential of a fine and loss of card privileges work to make companies compliant? To some extent, the answer is yes. A recent study by Verizon (leveraging its experience as a QSA company) found the number of companies rated as PCI-DSS compliant increased 80 percent from 2013 to 2014.[1] And the overall rate of compliance rose for 11 of the 12 PCI-DSS requirements. Only Requirement 11, covering testing, suffered a drop in companies able to meet the standard.[1]

But the total number of compliant companies is still relatively low. Significantly, the Verizon study also found that the vast majority of companies it surveyed were still noncompliant. While the failure rate had indeed dropped from the 2013 level of 88.9 percent, a year later, the rate of noncompliant companies was still a high 80 percent.[1]

What's more, Verizon found problems with sustainability. Less than a year after meeting all the PCI-DSS standards, 71.4 percent of compliant companies surveyed had fallen out of compliance.[1]

IBM has also asked a number of mainframe customers what they are doing about PCI-DSS compliance. Many said they had begun projects on a variety of platforms, but the mainframe is often not included—a concern considering that cardholder data is typically stored on the mainframe.

Using the mainframe to improve PCI-DSS compliance

In many of the large enterprises that PCI-DSS addresses, mainframes are the system of choice for hosting mission-critical payment card data and personally identifiable information. Organizations around the world—including 96 of the world's top 100 banks and 23 of the top 25 US retailers—trust their business to securable, scalable, self-optimizing IBM® z Systems™.[6]

Estimates are that mainframes process roughly 30 billion business transactions daily, including most major credit card transactions, stock trades and money transfers.[6] For database operations, 65 of the world's top banks and 24 of the 25 top US retailers run IBM DB2® on the IBM z/OS® operating system.[7]

The published requirements for PCI-DSS compliance, in fact, also recognize the inherent reliability of mainframes, describing their "ability to natively implement security" and noting that "systems that are commonly affected by malicious software typically do not include mainframes."[8]

Organizations that deploy z Systems mainframes have protection built in—including security in the processor, operating system, storage and applications. They can address security requirements such as identity and access management, hardware and software encryption, and event logging and reporting. This is what's known as a "highly-securable" system—all you have to do in order to secure the mainframe is take a few simple steps to implement functions and features that IBM provides.

The built-in ability of z Systems to encrypt data can also play a significant role in reducing the cost of a data breach. A study of all environments, including distributed, found that only 44 percent extensively use encryption to protect their data. It also found, however, that the use of encryption can reduce the cost of a data breach by USD12 for each stolen record.[4] What's more, with mainframe hardware encryption, not only is the data more secure, but the encryption has minimal impact on transaction processing performance.

Mainframes, as a result, are trusted across industries for their rigid standards, integrated hardware and software that enable security, integrity and high performance. But even organizations deploying mainframes must take steps to ensure they comply with PCI-DSS requirements. This is due in part to the growing role mainframes play in supporting vulnerable mobile applications, where many card purchases are made, and to mainframes' increasing use of data-sharing and interaction with less secure distributed systems inside and outside the enterprise.

Requirements organizations must meet for PCI-DSS compliance

Complying with each of the 12 PCI-DSS regulations

The increased number and sophistication of security threats—as well as the increasing reliance of businesses and consumers on payment card transactions over cash or check, especially for online mobile transactions—means that compliance with PCI-DSS standards will only become more critical over time.

Implementing mainframe security and privacy controls gives organizations the capabilities they need to protect, monitor, audit and report on compliance status and vulnerabilities as required by these standards. Built-in mainframe capabilities including z Systems encryption, and software solutions including IBM Resource Access Control Facility (RACF®), the IBM Security zSecure™ suite, the IBM Security Guardium® suite, IBM InfoSphere® Optim™ Data Privacy and IBM QRadar® Security Intelligence Platform give organizations the tools they need to better provide end-to-end security for their customers and their business.

1. Install and maintain a firewall configuration to protect cardholder data

The function of a firewall is to keep untrusted external networks from gaining access to sensitive information—in this case, cardholder data—on internal networks. A firewall isolates the payment card environment by blocking network traffic that doesn't meet security criteria, preventing traffic from making its way down pathways into key systems. In an IBM mainframe environment, isolation is accomplished by:

- Maintaining separation from the payment card environment in the z/OS logical partitions that manage PCI data, along with physical subnets, network adapters, virtual local area networks (LANs), TCP/IP stacks, ports and other key network components
- Further isolating the PCI environment using tools and tactics such as concealing networks, connection isolation, stack-affinity and bind-specific servers, SYSLOGD isolation, secure zones and a DMZ
- Implementing IBM Security Network Intrusion Prevention System appliances to protect against constantly evolving threats to the network
- Cryptographically protecting the network with secure network protocols and packet filtering to protect sensitive services from being accessed by unknown parties
- Installing IBM Security zSecure Audit and IBM Security zSecure Alert to verify and monitor security of the z/OS Communications Server

These measures are intended to achieve exactly what firewalls are designed to do: prevent unauthorized traffic from any external or internal source, whether ecommerce interactions, employee Internet access, dedicated business-to-business connections or wireless network traffic.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals often use vendor default passwords and other vendor default settings to gain access to secure information. In the IBM mainframe environment, protecting against this threat means:

- Employing solutions from the zSecure suite to flag and prevent default passwords, and some default settings
- Providing RACF password controls with the ability to change passwords and render default passwords inactive
- Enabling control over what programs are loaded into authorized program facility (APF)-authorized libraries, since APF-authorized programs can access functions that can affect system security and integrity

These capabilities—coupled with the establishment of robust organizational security standards and policies, adherence to processes for resetting passwords, keeping current on requirements, and establishing clear internal standards to follow—can inhibit the threat of fraudulent password access to data.

3. Protect stored cardholder data

The requirements for protecting stored cardholder data are clear: Keep cardholder data storage to a minimum. Retain only what is absolutely necessary to meet regulatory, legal or business requirements, and securely delete what's not necessary. Limit access to the cardholder's PAN by masking it when it is displayed and encrypting it when it is stored. And implement procedures to protect the keys that are used to secure stored cardholder data. In the mainframe environment, these points are addressed by:

- Including capabilities such as erase on scratch, which physically erases data when it is deleted, in order to ensure that the data is no longer readable
- Integrating the InfoSphere Optim Data Privacy solution, which provides capabilities to meet the requirements for masking data when it is displayed during test, development and analytical purposes; the solution retains the data's behavioral characteristics to make it look real while making data unreadable through encryption when it is stored or being transmitted; this is made possible by IBM InfoSphere Guardium Data Encryption for IBM DB2 and IBM Information Management System (IMS™) databases, and by the Encryption Facility for z/OS
- Protecting keys with Integrated Cryptographic Service Facility and Encryption Key Management Facility software that functions as an interface with the mainframe hardware where keys can be stored
- Protecting self-encrypting storage keys with IBM Security Key Lifecycle Manager software
- Use IBM Security zSecure Command Verifier to prevent changes to RACF definitions that protect the data

4. Encrypt transmission of cardholder data across open, public networks

Strong cryptography and security protocols are essential for safeguarding cardholder data when it is being transmitted over open, public networks. The IBM mainframe environment addresses this in a number of ways, including:

- Utilizing secure communication protocols such as IPSec, AT-TLS and other transmission protection protocols when transmitting payment information across open public networks
- Protecting information at the database level with Guardium data encryption, which uses z Systems cryptographic hardware to protect data in DB2 and IMS databases
- Using RACF to protect the data sets and other resources such as application source code in data sets
- Encrypting data at the device level using self-encrypting storage devices such as the IBM DS8000® storage devices with Full Disk Encryption, as well as encrypting data at the subsystem and application levels
- Using zSecure Audit to flag whether services such as FTP and TELNET allow data to flow in the clear

5. Protect all systems against malware and regularly update anti-virus software programs

Typically, mainframe operating systems such as IBM z/OS are not affected by malicious software. However, one of the hallmarks of malware is that it is constantly changing and often mutates into new forms that give rise to new vulnerabilities. For this reason, it is important that organizations establish a process to identify security vulnerabilities, protect against those vulnerabilities and take other steps to maintain secure systems and applications. Part of protecting against known vulnerabilities is staying current on malware threats by identifying new ones as they emerge, staying current with product releases, and updating configuration standards and processes to address them. A process that can be embedded into the vulnerability management program includes:

- Accessing IBM z Systems Security Portal to obtain Authorized Program Analysis Reports (APARs) containing information on security and system integrity for z/OS and the IBM z/VM® hypervisor
- Use zSecure Audit to verify whether operating system libraries are exposed in places where malicious code could be inserted by bypass security; zSecure Alert can also be used to monitor sensitive libraries

6. Develop and maintain secure systems and applications

Complying with this requirement is a matter of instituting a program of best practices for mainframe security that addresses each specific component of the PCI-DSS requirements. These practices include:

- Establishing a process to identify security vulnerabilities and scheduling regular audits to be sure the process is working; zSecure Audit can automate some of the tasks involved
- Installing vendor-provided security patches to protect against known vulnerabilities
- Instituting a program of best practices for secure development of internal and external applications
- Following change control processes and procedures for changes to system components, in an environment where production systems and development/test systems are strictly separated
- Training software developers in secure coding techniques, including the Payment Application-Data Security Standards (PA-DSS) to which applications in the PCI-DSS environment must adhere
- Documenting security policies and operational procedures and disseminating information about them to everyone across the enterprise

7. Restrict access to cardholder data, 8. Identify and authenticate access, and 9. Restrict physical access

These requirements fall under the general requirement to implement strong access control measures aimed at preventing anyone from accessing cardholder data without authorization. In a mainframe environment, measures to comply with these requirements can be categorized as measures for general security, database security and transactional security. These include:

- Using an installed external security manager (ESM) such as RACF and properly defining profiles for cardholder data-related resources such as data sets, commands, transactions, and user attributes and privileges; zSecure Admin and zSecure Audit can efficiently manage the ESM
- Having DB2 database grants in place for all cardholder-related table data and clearly defining and separating database administration roles
- Putting transaction security in place based on the appropriate classes and profiles in the context of the IMS transactional database management system or the IBM Customer Information Control System (CICS®) application server for transaction management capabilities
- Ensuring separation of duties for both systems and personnel to avoid conflicts in information access and excessive access for individuals

In addition, with regard to physical security, it is important to institute measures that restrict physical access to removable disks or tapes—and to any printouts of the information residing on the disks or tapes.

10. Track and monitor all access to network resources and cardholder data

Tracking and monitoring access requires an audit capability that makes it possible to exert full control, including the ability to activate monitoring for individual users. The IBM mainframe environment offers organizations multiple ways to achieve this level of control, specifically by:

- Activating RACF auditing for SPECIAL and root users, including for specific users of interest such as auditors, database administrators and system programmers
- Implementing protected automated audit trails for all system components to reconstruct user access to cardholder data, root or administrator user actions, and user and group management
- Using RACF to view and using zSecure solutions to print and report on system management records of activity—or using QRadar Security Intelligence Platform for enterprise-wide visibility into this information

11. Regularly test security systems and processes

Regular vulnerability and penetration testing are critical to compliance with PCI-DSS. Requirement 11 specifically calls for running network vulnerability scans at least quarterly—and after any significant changes are made to the network. It also calls for implementing penetration testing that is based on industry-accepted practices; extends to the entire perimeter and

critical systems; covers testing in and outside the network; and validates segmentation and scope-reduction controls. The IBM mainframe environment supports testing efforts by:

- Providing capabilities via IBM Security zSecure Audit to verify the effectiveness of security policies by analyzing system security information
- Providing capabilities via IBM Security zSecure Admin Access Monitor and RACF-Offline to test and simulate changes that impact the cardholder environment
- Providing zSecure Audit compliance testing for PCI-DSS to examine and report on the level of PCI-DSS compliance the organization has achieved

12. Maintain a policy that addresses information security for all personnel

PCI-DSS compliance relies on establishing, maintaining and sharing a strong information security policy that will provide clear guidance for implementing the security measures that are needed to protect cardholder data. Compliance also depends on all employees being aware of the sensitive nature of cardholder data and of their responsibility to protect it. Steps for putting these policies in place include:

- Establishing, publishing, maintaining and disseminating a security policy that includes a set of security standards that invoke industry best practices. These should be based not just on PCI-DSS requirements but also on:
  - Security Technical Implementation Guides (STIGs) from the National Institute of Standards and Technology (NIST)
  - The ISO/IEC 27001 standard for an information security management system (ISMS)
- Developing technology usage policies and defining proper use of critical technologies

Software solutions that support PCI-DSS compliance

IBM can help protect against threats and support PCI-DSS compliance with best-of breed security solutions. Capabilities build on a 50-year tradition of features such as encryption that are inherent to z Systems mainframes. Additional capabilities are provided by a portfolio of industry-leading IBM Security software offerings that are kept constantly up to date to meet today's changing threats.

- **Guardium suite:** Helps protect many enterprise-wide data sources with continuous, policy-based, real-time monitoring of data traffic activities, including actions by privileged users. Provides automated blocking of data with automated workflows to support regulatory compliance and vulnerability assessment—as well as identification, classification and encryption of sensitive/personally identifiable information.
- **zSecure suite:** Provides automated and integrated solutions for z/OS-based systems via security analysis, threat detection, problem remediation, user provisioning, security policy enforcement, compliance auditing and enterprise-wide security intelligence.
- **zSecure Audit compliance testing for PCI-DSS:** Automates collection, analysis and reporting of specific PCI-DSS compliance information to show users in an easy-to-understand format the percentage level of compliance they have achieved.
- **QRadar Security Intelligence Platform:** Provides a unified architecture for integrating security information and event management, log management, anomaly detection, incident forensics and configuration, risk management and vulnerability management.
- **RACF:** Integrates with the mainframe's built-in security features to enhance data security. Identifies, verifies and authorizes system users; identifies and classifies system resources; logs and reports attempts at unauthorized access; protects data resources by controlling access.

- **IBM Security Key Lifecycle Manager:** Provides a single point of control, policy management and reporting to simplify encryption key security lifecycle management. Integrates with IBM storage systems to address PCI-DSS regulations that call for strong protection of encryption keys.
- **Integrated Cryptographic Service Facility:** As a software component of z/OS, works with RACF and the hardware cryptographic feature of z Systems to provide the application programming interfaces (APIs) by which applications request and achieve high-speed encryption.
- **IBM Security Identity Manager and IBM Security Privileged Identity Manager:** Automate the creation, modification, recertification and termination of identities throughout the user lifecycle to drive effective identity management and governance for improved security and compliance.
- **InfoSphere Optim Data Privacy:** De-identifies confidential data on demand throughout the enterprise including big-data platforms. It masks data statically or dynamically in applications, databases and reports across production and nonproduction environments.

Conclusion

IBM mainframes provide a platform with built-in security capabilities, and IBM Security software solutions provide industry-leading security management capabilities to help organizations mitigate payment-card related risk and comply with the structured requirements of the PCI-DSS program. For organizations that utilize payment cards in their business, these solutions can help avoid noncompliance penalties assessed by the PCI Security Standards Council. More importantly, they can help avoid the costs of data loss and breach remediation that continue to rise. All of these solutions combine to make z Systems an ideal platform for PCI-DSS processing.

For more information

To learn more about IBM Security solutions for mainframe environments, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

[1] Ciske van Oosten et al., "Verizon 2015 PCI Compliance Report," *Verizon*, March 9, 2015. http://www.verizonenterprise.com/pcireport/2015/

[2] Jessica Silver-Greenberg et al., "JPMorgan Chase Hacking Affects 76 Million Households," *The New York Times*, October 2, 2014. http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0

[3] "20 Million People Fall Victim to South Korea Data Leak," *Security Week*, January 19, 2014. http://www.securityweek.com/20-million-people-fall-victim-south-korea-data-leak

[4] "2015 Cost of Data Breach Study: Global Analysis," *Ponemon Institute*, May 2015. http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

[5] "PCI-DSS: Security-Penalties," *University of California at Santa Cruz*, Accessed May 27, 2015. https://financial.ucsc.edu/Pages/Security_Penalties.aspx

[6] Janet Sun, "Don't Believe the Myth-information about the Mainframe: Part 1," *SHARE*, May 07, 2013. http://www.share.org/p/bl/et/blogid=2&blogaid=234

[7] Source: 2013 IBM zEnterprise Technology Summit

[8] "Navigating PCI DSS, Understanding the Intent of the Requirements," *PCI Security Standards Council*, October 2010. https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf

WGW03125-USEN-00