PCI Data Security Standard

A Pathway to PCI Compliance

TABLE OF CONTENTS

EXECUTIVE SUMMARY

During the last ten years there has been an explosion in the use of Internet-based commerce, as well as a drastic increase in credit and debit card usage in the physical storefront. Despite the best efforts of organizations to protect customer data, consumer fraud and identity theft have hit new highs. According to the U.S. Department of Justice, the number of identity thefts and fraudulent credit card charges reached over four million in the U.S. in 2006. In response to this increased threat, governments around the world have been considering an array of new laws and regulations to systematically combat the problem. In addition, the banking and credit card industry have spearheaded their own initiatives, including the newly revised Payment Card Industry (PCI) Data Security Standard (DSS). This standard was developed to provide all organizations that deal in credit card transactions with the best tools to combat growing security threats.

As is true anytime we tighten security and policy, there is the potential for a corresponding increase in user complexity and decrease in productivity. A key to success with any regulatory compliance effort is to accomplish measurable goals using policy and controls that are easy for the users to implement and accept. Better usability ensures acceptance and compliance, resulting in better security. Complex, arduous solutions are doomed to user rejection and ineffectiveness.

This paper will examine some of the requirements of the new standard and review identity and access management technology that can help organizations comply with these regulations in an efficient and cost-effective manner that is easy for users to embrace.

WHAT IS PCI?

In September of 2006, American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International banded together to form an independent council designed to recommend sound data security practices that would protect consumer privacy. The council developed the Payment Card Industry (PCI) Data Security Standard (DSS), the - first standard in the industry to focus on improving payment account security throughout the transaction process. In addition, the recommendations of the council are designed to provide credit card processors, point-of-sale vendors and financial institutions with a concise, cohesive approach to data security. Ultimately, more than one billion global payment card users will benefit from stronger security at all points of the transaction process, lessening the chance of individual data theft.

The PCI-DSS contains 12 general requirements that are designed to:

- Build and maintain a secure network;
- Protect cardholder data;
- Maintain a vulnerability management program;
- Implement strong access control measures;
- Regularly monitor and test networks; and
- Maintain an information security policy

These broad-based recommendations are backed by a host of specific technical recommendations which are designed to help guide vendors in their selection and implementation of various data security technologies. As with any solutions guideline, there are no magic bullets, and many different approaches can be used to help achieve information security compliance.

PCI STANDARDS AND IMPACT ON GLOBAL BUSINESS

The goal of the PCI standard is to make electronic commerce universally safer and easier to implement for the banking and electronic credit card industry. To adhere with the new regulations, all merchants in the transaction chain must comply with the same standards, although some allowances are given based on the size of the business. The goal of the PCI committee is to make security compliance achievable by all organizations regardless of their size.

BEST PRACTICES FOR COMPLYING WITH PCI REGULATIONS

PCI-DSS was designed to protect the privacy of customers, and payment card and merchant data at the point of sale (POS), in transit, and at rest. Companies that can demonstrate compliance with the PCI standard and prove that they are trustworthy custodians of customer data have the opportunity to build solid customer loyalty. Complying with PCI regulations is challenging because the required security measures span the network and attached systems. Most industry experts agree that the best way to achieve and maintain PCI compliance is to adopt a strategic and pragmatic approach to locking down their networks. This includes the ability to centrally manage systems, network services, and provide user access to critical systems based on individual access rights. The six main pillars of the new information security standards are intended as a guide for companies to implement the new PCI standards.

PCI DATA SECURITY STANDARDS

The new Data Security Standard is comprised of a number of security requirements, each one of which is designed to protect consumer data while at rest and in motion. A solution that incorporates single sign-on and strong authentication with policy enforcement and central reporting can help cover many of these requirements, several of which follow:

1. Build and maintain a secure network

Requirement: Do not use vendor-supplied defaults for system passwords and other security parameters

In both the banking and the retail environment, all systems must be protected from unauthorized access from the Internet. PCI requires that organizations do not use vendor supplied defaults for system passwords. It is well known that hackers often try to use default passwords to gain access to unauthorized areas of a system.

Today's complex business environments also often include multiple systems requiring many different passwords. Even in cases where the default password is not used, users will often choose one simple password (often well-known) to access several different applications, an inherently insecure practice. If multiple passwords are required, users will often write them down where they could be discovered by unscrupulous users. Therefore, it is recommended that if passwords are used they should be private, unique, adequately complex, and with changes automated, greatly reducing the potential for misuse or theft.

Solution: With Imprivata OneSign® Single Sign-On, administrators can implement a clear, straightforward password policy across all SSO-enabled applications based on users' primary authentication. So, users can be granted access to only those areas for which they are authorized. For additional security, OneSign is able to cycle complex application passwords behind the scenes on the users' behalf. This allows organizations that require certain application passwords to be changed periodically to handle the changes automatically without user effort; and in fact the users no longer need to know the application passwords. This feature is crucial in complying with the new data security policy which recommends frequent password changes. In addition, OneSign can easily replace traditional network passwords with a range of strong authentication options; such as smart cards, one-time password tokens, and biometric readers.

2. Implement strong access control measures

Requirement: Restrict access to cardholder data by business need-to-know

Requirement: Assign a unique ID to each person with computer access

Requirement: Restrict physical access to computer data

In today's open networks, it is often difficult to maintain access control over varied and wide-reaching systems. This is why the PCI data security panel highly recommends implementing strong access control measures across the computing environment. In any IT environment there should be a system that:

- Establishes a mechanism for systems with multiple users that restricts access based on a user's need to know and is easy to set to "deny all" unless specifically allowed access to the system.
- Limits access to computing resources and cardholder information only to those individuals whose jobs requires such access.
- In addition, it is recommended that each user be assigned a unique authentication method, ideally a token device, smart card or biometric that can provide strong two-factor authentication to the systems.

Solution: Imprivata's single sign-on solution allows users to easily access the systems needed to be productive only if users have the proper credentials. Through the use of policy settings, Imprivata's solution can restrict user access to any system, without adding a complex, cumbersome user login workflow. Users can log onto a system once based on policy, using a set of approved credentials and then initiate a more secure, better monitored access to any required applications.

A range of authentication methods can be employed to provide the appropriate controls and assurances that the user is authentic and accountable. One of the crucial aspects of compliance with the new PCI Data Security standard is the ability for organizations to ensure that only those "approved" users have access to sensitive cardholder data. Authentication methods such as passwords, finger biometric identification, active and passive proximity cards, smart cards, onetime-password tokens, USB tokens are recommended to ensure adequate levels of assurance that users "are who they say they are".

Imprivata OneSign's SSO capabilities can combine with its ability to link physical and IT security systems to consolidate identities between physical access systems. The awareness of a user's location or facility access card status when combined with their other authentication credentials provides an even higher level of user authentication assurance and monitoring.

3. Regularly monitor and test networks

Requirement: Track and monitor all access to network resources and cardholder data

Requirement: Regularly test security systems and processes

Networks are continually changing; therefore it is crucial that organizations have logging mechanisms in place that can track the activities of users. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. However, even armed with a set of common system logs, determining the cause of a breach and then recommending appropriate action can be impossible at worst, and extremely difficult at best.

This solution can provide consolidated reporting of networks and corresponding physical areas that have been accessed. IT staff can easily pull reports that for the first time consolidate the application and network access events across all applications and across all computers in a useful policy enforcement context. In cases where the physical access control system has been combined with the solution, the administrator also gets a comprehensive view of the user access including policy enforcement based on badge status, location, remote access attempts, and more.

Solution: By implementing a OneSign SSO solution, organizations can track and monitor all access to systems housing cardholder data. OneSign records all events in log files that are accessible to the administrator, and includes a history of all OneSign configuration changes with a timestamp/username of the administrator for audit purposes. Client-side SSO events are collected and consolidated by the OneSign appliance for centralized viewing/reporting of relevant events on a per-user, per-computer, or aggregate basis. All user login, password change, session start-stop, and success and failure events are centrally consolidated in the appliance for powerful reporting.

In addition, integration of SSO with physical and IT security systems gives the added benefit of being able to view user activity in a timeline including facility entry, computer access, and application access; all from one central location. As users are granted access to certain computing areas, their physical access to computers in these areas can also be controlled and monitored by OneSign's location based authentication. This provides PCI compliance of monitoring and protecting areas that house cardholder data.

4. Maintain an information security policy

Requirement: Maintain a policy that addresses information security

As new security procedures are put in place it is important to also institute a process for maintaining and updating security policies that match security objectives. At a minimum, policies should be reviewed on an annual basis, and it is also recommended that a specific security team be assigned to:

- Establish, document and distribute security policies
- Monitor and analyze security alerts and information, and distribute to appropriate personnel
- Administer user accounts, including additions, deletions, and modifications
- Monitor and control all access to data

Solution: With OneSign Single Sign-On administrators decide which users should have which authentication modes, and whether they should upgrade their authentication options over time. Authentication policy represents just the first step in ensuring that correct and appropriate user access controls are in place to protect cardholder data. Application-level password policies are important as well to allow implementation of complex password change policies without overburdening the users to the point they must "cheat" or reject the policy entirely.

In addition, the OneSign Intelligent Agent™ allows organizations to monitor, capture and log user access events in a centralized database. Easy-to-use detailed reporting can strengthen security and enforce policy compliance across all applications. Administrators can easily monitor access records for every user, application or workstation in one central location - even revealing users that are sharing credentials to access critical applications. The monitoring of all access to credit card data is an essential part of the new Data Security Standard and can provide administrators with better controls and policy enforcement to help protect cardholder data.

OneSign allows for the creation and deployment of a single, converged security policy for allowing or denying remote or local network access based on a user's physical location, user role, and/or employee status. Policies can enforce authentication options, desktop locking behavior, and can be applied on a per-user, per-group, or per-computer basis for complete flexibility.

Event notifications are also important for near real-time response to suspicious or alarm conditions. OneSign includes the ability to automatically notify administrators in the event that a pre-configured condition is met. For example, notifications can be triggered for any after-hours failed login attempt, or any user lockout after too many failed login attempts have been recorded.

WHERE IMPRIVATA ONESIGN APPLIES TO PCI COMPLIANCE EFFORTS

Single Sign-On - Authentication Management – Physical/Logical Security Convergence

Imprivata OneSign technology gives organizations a simple, yet powerful tool for complying with the vast majority of emerging PCI regulations. Unlike other technologies on the market, OneSign is affordable and easy to install and administer and provides monitoring information with detailed reporting capabilities.

Payment Card Industry Data Security Standards	Imprivata OneSign
Build and Maintain a Secure Network	
Install and maintain a firewall configuration to protect cardholder data	
Do not use vendor-supplied defaults for system passwords and other security parameters	X
Protect Card Holder Data	
Protect cardholder stored data	
Encrypt transmission of cardholder data across open, public networks	
Maintain a Vulnerability Management program	
Use and regularly update anti-virus software	
Develop and maintain secure systems and applications	
Implement Strong Access Control Measures	
Restrict access to cardholder data by business and need-to-know	X
Assign a unique ID to each person	X
Restrict physical access to cardholder data	X
Regularly Monitor and Test Networks	
Track and monitor all access to network resources and cardholder data	X
Regularly test security systems and processes	X
Maintain an Information Security Policy	
Maintain a policy that addresses information security	X

IMPRIVATA ONESIGN, ADDRESSING MANY PCI REQUIREMENTS

Imprivata OneSign directly addresses many of the requirements of the new PCI Data Security Standard by combining single sign-on, strong authentication, reporting, and tight integration with physical access control systems.

Imprivata OneSign Single Sign-On uses patent-pending technology that enables SSO without modifying existing applications. Utilizing an appliance-based approach, Imprivata's single sign-on solution not only provides complete SSO functionality but has the additional security of being a hardened system onto itself. Organizations can benefit from centralized password administration, lower helpdesk costs, increased user productivity and satisfaction, and ability to demonstrate compliance.

OneSign requires no modifications to existing applications. With integrated support for multiple, strong authentication methods and centralized password policies, OneSign allows companies to implement levels of security that are appropriate for their environments.

OneSign is invaluable to IT departments managing a heterogeneous portfolio of applications. Because OneSign replaces multiple passwords and application logon events with a single, centrally-managed user logon, IT's burden is significantly reduced and usability is enhanced.

OneSign's browser-based tools allow administrators to increase information security through straightforward password policy settings, and administrators can change password constraints (minimum/maximum length, reset intervals, auto resets) to satisfy PCI and other regulations. They can also manage authentication challenges, and accommodate application-generated password reset requests—automatically saving organizations time and money.

ADVANTAGES OF SSO AND STRONG AUTHENTICATION IN THE MERCHANT ENVIRONMENT

E-commerce environments are as varied as the store fronts and electronic sites that house them. The result is a difficult user experience and a system that is fraught with security challenges and holes. In order to comply with many of the regulations set forth in the PCI Data Security Standards, organizations need to consolidate the administration of password and or strong authentication management. Imprivata OneSign SSOallows companies to consolidate password management and closely guards consumer data by allowing companies to set policy to ensure they can control access of corporate users to only those areas that they are authorized to access. This system can seamlessly integrate with most two-factor authentication solutions and most physical access security systems, providing for additional security right down to the physical access points.

IMPRIVATA – PROVIDING THE TOOLS FOR PCI COMPLIANCE

Complying with new regulations can be challenging for any business and the new standards set forth by the payment card industry will be equally, if not more challenging due to the scope of the requirements. Complying with these new standards in a timely and cost-efficient manner will require that companies look at solutions that are:

- Simple to install and administer
- Not intrusive to the existing network and security environment
- Easy for administrators and users to work with
- Cost-effective

Imprivata OneSign gives organizations a robust, yet simple and easy to install, SSO and strong authentication solution that provides key components for PCI compliance. In addition, Imprivata's OneSign Physical | Logical can provide authentication on the physical level that is not currently offered by any other vendor in the marketplace. Combined, these solutions provide companies with valuable tools to help comply with a majority of the current PCI regulations.

For more information on the PCI Data Security Standards you can go to:
https://www.pcisecuritystandards.org

To learn more about Imprivata OneSign, visit www.imprivata.com.

Offices In:
Belgium • Germany
Italy • Singapore
UK • USA

1 877 ONESIGN
1 781 674 2700
www.imprivata.com

WP-PCIC-Ver3-0808