White Paper

Achieving PCI Data Security Standard Compliance through Security Information Management

netForensics®

Contents

netForensics®

Executive Summary

Assuring the integrity and security of credit card information has been an ongoing challenge for companies with responsibility for consumer credit card information. In 2005, however, information security accountability intensified for merchants and payment service providers when the Payment Card Industry (PCI) Data Security Standard was introduced worldwide. MasterCard, Visa, and other major credit card corporations collaborated in developing the PCI standard to enable a single, consistent approach to safeguarding sensitive data for all card brands. By adhering to security standards on how cardholder data is handled and stored, retailers and service providers can help reduce debit and credit card fraud.

Strict PCI requirements compound existing information security responsibilities, so developing and implementing an effective security management system presents new challenges for organizations, consuming valuable resources in the process. Visibility into real-time threats and vulnerabilities is called for, yet most organizations lack the comprehensive data protection tools, performance measurement capabilities, and validation processes needed for both internal and external information security initiatives such as PCI compliance. Retailers and service providers must prove diligence in managing cardholder information security risk, or can face tough consequences including sizeable fines and even imprisonment.

Security information management (SIM) can enable merchants and service providers to protect cardholder data while managing ongoing security policies and procedures. By deploying netForensics' nFX Open Security Platform (nFX OSP), with its inherent SIM technology, organizations can transform security-related information into actionable security intelligence. Equipped with broad security knowledge, organizations can meet PCI security requirements and successfully address other industry regulations as well.

Introduction: Brief Overview of PCI

In 2005, Visa and MasterCard collaborated in creating common industry security requirements to help alleviate debit and credit card fraud. Based largely on Visa's Cardholder Information Security Program (CISP) and MasterCard's Site Data Protection (SDP) standards, PCI is now the worldwide standard for consumer data protection across the payment industry. Visa currently maintains the PCI standard and compliance program. PCI requirements apply to members, merchants, merchant banks or acquirers, and payment service providers that process, store, or transmit credit card information. According to the PCI standard, these security requirements apply to:

> *"…all 'system components' which is defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, Web, database, authentication, Domain Name Service (DNS), mail, proxy, and Network Time Protocol (NTP). Applications include all purchased and custom applications, including internal and external (Web) applications."* [1]

Thus, an enterprise-wide information security program that encompasses all network security devices, applications, and databases is necessary. Otherwise, organizations can face detrimental consequences for non-compliance, with sizeable fines per data theft

incidence, punitive damages, revocation of a company's right to accept or process credit cards, loss of consumer and partner confidence, and even imprisonment. Third-party service providers must also meet PCI compliance, since PCI requires merchants to only do business with service providers that adhere to the payment card security standards. To achieve compliance, merchants and service providers that handle a large number of transactions must pass quarterly and annual audits by a certified third-party assessor.

The PCI Challenge: Protecting Credit Card Information

As detailed in the PCI Data Security Standard manual, all merchants and service providers are required to meet the following objectives to adequately protect credit card information:

- Build and maintain a secure network — Install and maintain a firewall configuration to protect data; refrain from using vendor-supplied defaults for system passwords and other security parameters.
- Protect cardholder data — Protect stored data; encrypt transmission of cardholder data and sensitive information across 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 data by business need-to-know; assign a unique ID to each person with computer access; restrict physical access to cardholder data.
- Regularly monitor and test networks — Track and monitor all access to network resources and cardholder data; regularly test security systems and processes.
- Maintain an information security policy — Maintain a policy that addresses information security.[1]

Once these PCI compliance objectives are met, merchants and service providers must validate their efforts. The more transactions and account information a merchant or service provider processes, the more stringent the validation requirements. The largest credit card providers, Visa and MasterCard, have the toughest validation standards, which include an on-site security audit, a self-assessment questionnaire, and a network scan. Protecting the most sensitive customer information involves both monitoring external network activity as well as managing internal user activity at the application and database level. Much of the cardholder data is maintained in internal databases and application servers where threats often occur. These internal networks are comprised of many proprietary applications with vulnerabilities that can be difficult to identify and fix. Countless mission-critical hosts, though legitimate, may also pose a security risk. Additionally, IT teams must adequately maintain PCI compliance without blocking authorized data access or disrupting business processes. Given the complexities of protecting credit card numbers and other sensitive cardholder data from loss or compromise, an effective and comprehensive information security program must be implemented.

Security Information Management: The Foundation that Enables PCI Compliance

SIM can provide a flexible, scalable, and comprehensive solution for addressing risk management and PCI compliance challenges. An enterprise-class SIM solution can transform all information security-related data into actionable security intelligence. Properly

implemented, a best-practices SIM solution gives merchants and service providers real-time visibility into cardholder security-related risk and compliance data so that PCI standards can be upheld. Additionally, leveraging a SIM platform to comply with PCI can create a more reliable, streamlined IT infrastructure, improve service delivery, increase availability, and reduce risk. Organizations can also benefit from simplified auditing, more effective cost controls, and improved customer confidence and loyalty.

Assuming the following responsibilities to prove diligence in managing information security risk helps merchants and payment service providers meet PCI requirements, as well as those of other privacy and security regulations:

- Define a policy-driven security management program that can be incorporated early on into business processes — Identify the people and technology controls needed to satisfy the organization's security mission and ensure compliance. Also, ensure that security initiatives are integrated into business processes at their onset, rather than after the fact.
- Validate security controls — Provide for the monitoring and reporting of controls on human actions and decisions, process controls, and information technology controls.
- Implement a risk management approach to information security — Comprise active monitoring of risk as defined and measured by key control indicators (KCIs) and key risk indicators (KRIs), correlating the relative value of information assets, the threats to the confidentiality, integrity, and availability of the assets, and the vulnerability of the systems and architecture that store and carry the assets.
- Demonstrate due diligence in the application of internal controls — Create a link between the security infrastructure and policy by capturing all security events from all network hosts, devices, and assets in an auditable database.
- Develop and implement an effective security-incident management process — Demonstrate that the proper steps were taken to correct systems and adjust policy if a non-compliant situation is identified.
- Enable reporting that can help demonstrate compliance — Demonstrate the ongoing security of compliance-related assets over a period of time, recreating the organization's security posture in the event of an audit, and enabling security performance management against metrics that can be leveraged for corporate governance initiatives.
- Establish capabilities for archiving and data preservation — Preserve near-term and long-term data in its purest form for forensics and evidentiary presentation.

By implementing effective, comprehensive policies and procedures for establishing accountability and consistent reporting practices, retailers and payment service providers can successfully meet PCI regulatory compliance directives.

The netForensics Solution: Aligning with PCI Objectives

netForensics provides the SIM infrastructure to successfully address PCI compliance challenges. The nFX OSP set of security solutions provides organizations that store, process, or transmit cardholder data greater visibility, better intelligence, and more effective response to threats. The enterprise-class SIM technology from netForensics includes the following tools and technologies:

- Actionable Security Intelligence — With broad security intelligence, merchants and payment service providers have a foundation from which to maintain PCI compliance operations. Organizations can establish a continuous process of threat collection, identification, and remediation, and ensure business continuity.
- Enterprise-Class Security Decision Support — Organizations can meet compliance requirements through automated threat identification, by reporting against controls, and via incident resolution management. Additionally, they can resolve incidents as they occur. Metrics enable Performance measurement, with is enabled, with metrics to provide baselines for security and performance gauges at the analytical and executive dashboard levels.
- Scalable, Robust SIM Architecture — A scalable SIM architecture cost-effectively supports growth and reduces total cost of ownership in mid-size to large environments. The SIM architecture incorporates data from security and network devices, applications, scanners, and databases to deliver global visibility into all security-related activities, regardless of numbers.
- Correlation Technology and Processing Power — A comprehensive correlation technology goes beyond simply logging security information, and instead speeds threat identification and provides an accurate picture of risk. The nFX OSP technologies are architected to handle the massive volume of security information from network-related sources as well as server logs, applications, databases, and identity management systems, and pinpoint attacks from the inside and beyond based on a thorough understanding of network and user activity. The correlation technologies process large volumes of data from the perimeter down to the core to identify real-time threats and historical patterns.
- Visualization, Reporting, and Analytics — Merchants and service providers can visualize threats as well as the security information underlying the threats. Through the in-depth reporting functionality, key stakeholders and especially auditors have ready access to comprehensive PCI compliance data. The deep level of analytics enables organizations to measure compliance, risk, and operational performance so that security analysts, operators, and executives can determine the security posture and take any necessary steps to improve it.
- Incident Resolution Management Workflow and Embedded Security Knowledge — nFX OSP offers guidance through a repeatable incident response workflow, allowing firms to effectively eradicate threats and prevent reoccurrences. Through actionable security intelligence, the incident remediation process is documented for security policy management and improvement purposes, as well as for regulatory audits. The embedded knowledge base integrates third-party security information that includes a pre-populated database of incidents and how to resolve them.
- Application Security Monitoring — nFX OSP, designed with monitoring at the application layer, provides comprehensive application security monitoring at the application layer. Flexible deployment options allow nFX OSP to be configured optimally to handle application events, while failover and redundancy guarantee the availability of events from identity management systems, server logs, and traditional network security devices. Dashboards and reports allow everyone involved in the process of enterprise security to understand the impact of an application-level incident on business continuity.

With these SIM tools and technologies, merchants and payment service providers can effectively manage information security risk and demonstrate PCI compliance.

Conclusion

Like government mandates such as Sarbanes-Oxley (SOX) and the Gramm-Leach-Bliley Act (GLBA), PCI requires IT organizations to take a close look at existing security information strategies and identify any gaps that could prevent regulatory compliance. Protecting cardholder information involves addressing the risks associated with countless system components, including network devices, servers, and applications. Merchants and payment service providers must implement broad policy-driven security programs to reduce the overall risk associated with storing, processing, or transmitting cardholder data in order to address PCI requirements.

A SIM solutionsystem like nFX OSP, along with alignment of people, processes, and technology, enables retailers and payment service providers to meet PCI objectives and ensure a resilient infrastructure. SIM enables companies to leverage existing technology and tools to identify, assess, and report on security-related issues and events for cardholder data, and ultimately provide tangible evidence of their efforts.

References

1. Payment Card Industry Data Security Standard,

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf

2. Health Insurance Reform: Security Standards — Final Rule,

http://a257.g.akamaitech.net/7/257/2422/14mar%2020010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf

About netForensics

netForensics transforms all security related information into actionable intelligence, enabling more than 450 enterprises and government agencies to better respond to security threats, maintain compliant operations, and ensure the continuity of key business processes.

By harnessing the power of our award-winning Security Information Management platform that manages more security events at more organizations than any other product in the marketplace, we help customers deliver security management solutions that rely on the availability of timely and relevant information security information.

We facilitate these actionable security intelligence (ASI) solutions by rationalizing security information from strategic applications and critical compliance-related assets, as well as the perimeter devices that protect them. ASI solutions make this information available to technology domains and users within the security organization and beyond — by unifying network and security organizations, while supporting IT governance, enterprise compliance, and risk management initiatives.

200 Metroplex Drive • Edison, NJ 08817 • p 732.393.6000 • f 732.393.6090
www.netforensics.com • info@netforensics.com