Achieving ROI From Your PCI Investment

White Paper

November 2007

Contents

The Payment Card Industry Data Security Standard (PCI DSS) affects organizations of all sizes and types, from financial institutions to retailers and hotel chains. Covering such diverse areas as physical security, encryption and access control, compliance with the PCI DSS represents a significant and long-term commitment of resources by those organizations involved.

However, what is becoming clear is that as part of the compliance process, businesses are beginning to see opportunities to realize a measurable return on the investment involved.

This short whitepaper discusses both the challenges of meeting PCI DSS compliance, as well as the ways in which organizations can leverage that work to provide better security, more easily meet future compliance requirements, and create operational efficiencies within their IT organization.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, Provider-1, SiteManager-1, and VPN-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, AppAnalyzer, Application Scanner, AppManager, AuditTrack, Chariot, ClusterTrends, CommerceTrends, Configuration Assessor, ConfigurationManager, the cube logo design, DBTrends, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, End2End, Exchange Administrator, Extended Management Pack, FastTrends, File Security Administrator, Firewall Appliance Analyzer, Firewall Reporting Center, Firewall Suite, Ganymede, the Ganymede logo, Ganymede Software, Group Policy Administrator, imMarshal, Intergreat, Knowledge Based Service Assurance, Knowledge Scripts, MailMarshal, Marshal, Migrate.Monitor.Manage, Mission Critical Software, Mission Critical Software for E-Business, the Mission Critical Software logo, MP3check, NetIQ, the NetIQ logo, the NetIQ Partner Network design, NetWare Migrator, OnePoint, the OnePoint logo, Operations Manager, PentaSafe, PSAudit, PSDetect, PSPasswordManager, PSSecure, Qcheck, RecoveryManager, Security Analyzer, Security Manager, Security Reporting Center, Server Consolidator, SQLcheck, VigilEnt, Visitor Mean Business, Vivinet, W logo, WebMarshal, WebTrends, WebTrends Analysis Suite, WebTrends for Content Management Systems, WebTrends Intelligence Suite, WebTrends Live, WebTrends Log Analyzer, WebTrends Network, WebTrends OLAP Manager, WebTrends Report Designer, WebTrends Reporting Center, WebTrends Warehouse, Work Smarter, WWWorld, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Introduction

According to Business Trends Quarterly[1], during 2006 the rate of exposure of personal information averaged 6 million records per month. High profile events such as the TJX data theft (at least 45 million records lost)[2] and a constant stream of stories regarding insider theft and poor security processes have sharply eroded consumer confidence in the security of their personal information. This, in turn, has cost retailers significant revenue opportunities. One study by Gartner has put the lost opportunity cost for 2006 at around $2 billion.

As part of a long-term effort to restore confidence, the major credit card processing organizations, including VISA, MasterCard and American Express, are requiring companies that handle credit card data to implement and enforce strict controls on data security, their infrastructure, and the processes and personnel involved. These controls are defined in their Payment Card Industry Data Security Standard (PCI DSS) initiated in 2004 and with a series of deadlines in 2007 and 2008. (The 12 major requirements for PCI DSS are listed in Appendix A).

With little choice but to comply, many retailers and financial institutions are working towards implementing the 12 broad requirements contained in PCI DSS. However, rather than seeing compliance as an additional burden on already overstretched IT resources, some organizations are now finding opportunities to leverage their PCI DSS compliance efforts to generate long-term return on investment.

Difficulties in Compliance

The PCI DSS requirements range from being relatively simple to implement, such as ensuring up-to-date anti-virus software, to complex and demanding procedural changes such as tracking and monitoring access to network resources and cardholder data.

The requirement to eliminate vendor-supplied passwords (requirement 2 of PCI DSS), for example, can be extraordinarily difficult to consistently enforce and document. Implementation may cross many departmental boundaries, potentially involve several teams, and affect multiple system platforms. Such efforts can be both time consuming and expensive. Worse, studies show that organizations usually underestimate the initial difficulty and cost of implementing PCI DSS.[3]

It's hardly surprising then, that according to an October 2007 Wall Street Journal article, compliance rates are low. "Merchants, unfortunately, have been slow to respond. Of the 327 largest merchants, just 44% of them have validated their compliance, according to Visa."[4]

Organizations are asking not only how to best drive compliance efforts with the least financial and business impact, but increasingly asking how to leverage those efforts to maximize the return on investment.

[1] Business Trends Quarterly: "Security Compliance: Are you your own worst enemy?" – Barclay T. Blair.

[2] http://www.usatoday.com/money/industries/retail/2007-03-29-tjx-id-theft_N.htm TJX discloses largest data theft: 45.7M customers

[3] Aberdeen Group: Protecting Cardholder Data – June 2007

[4] Wall Street Journal. Online at http://online.wsj.com/article/SB119161871891550536.html?mod=googlenews_wsj

Achieving Compliance

Before they can reach compliance, however, organizations must undertake a substantial review of their current compliance posture. Tools that perform vulnerability scans, especially when clearly tied to extensive compliance knowledge bases can be especially beneficial. For example, NetIQ Secure Configuration Manager® can be used to readily discover network assets, scan them for known vulnerabilities and, in the case of PCI DSS Requirement 2, ensure that vendor defaults are not being used. It can also report on compliance with security configuration standards, such as the Center for Internet Security benchmarks that are recommended by PCI DSS.[5]

Once such a pre-compliance audit is complete, then a more focused planning effort can be undertaken, with particular emphasis on those areas in which is it typically more difficult to achieve compliance, such as Requirements 3, 11, 8, 10 and 1.[6]

While most organizations typically report initial compliance efforts taking from 12 months to 18 months[7], attaining compliance is not the end of the story.

Maintaining Compliance

Many of the control objectives in PCI DSS are really process objectives and can not be attained by simply establishing a new set of hardware or software technology. For example, while Requirement 8 mandates at a broad level that each user is assigned a unique ID, there are long-term processes that must be in place to maintain this. Section 8.5.5 mandates that inactive accounts are removed after 90 days, and 8.5.6 requires remote maintenance accounts used by vendors to be active only for limited periods when necessary. Ensuring that these processes are not only initiated, but also that they continue to be enforced requires a systematic and often automated set of procedures.

Further, not only must these processes be put in place, they must also be clearly documented and visible for auditors to ensure that compliance in maintained. Once compliance has been reached, however, opportunities exist to capitalize on the invested effort.

Making PCI Work for You

Estimates vary for the number of organizations that have already reached full compliance. What is undeniable is that a very large number of companies are investing considerable time and resources into complying with the necessary PCI DSS standards.

Although this effort is being driven primarily by the need to achieve the 12 PCI DSS requirements, what is also becoming apparent is that many organizations are seeing their compliance efforts as providing much broader benefits than may initially have been expected. Indeed, such benefits straddle many areas of the organization, not just those concerned with the handling of credit card information.

To understand why this is, consider two significant driving forces behind much of the adoption of new security technology. The first force has been the explosive growth both in the numbers and the public awareness of attacks aimed at stealing data. Targeted data goes beyond credit card data to other customer information, individually identifiable health information, trade secrets, and more.

[5] A complete mapping of NetIQ’s security solutions to the PCI DSS standard they enable is provided in Table 1 and a functional mapping appears in Appendix B

[6] Guide to passing PCI's five toughest requirements, Craig Norris 09.19.2007. Online at http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1271917,00.html

[7] Aberdeen Group: Protecting Cardholder Data – June 2007

The second force is the legislative response driven by these attacks, including new regulations at the federal, state and even international level. These include Health Insurance Portability and Accountability Act (HIPAA) and other privacy laws, but also several states that are mandating PCI DSS as law.[8]

Further, attacks aimed at misusing data, specifically fraud, continue to grow in seriousness and frequency. According to the 2007 CSI Computer Crime and Security Study[9], fraud now represents the most costly form of attack reported, and insider incidents (network abuse, etc) are now the most frequent incidents reported.

How PCI DSS Can Provide a Significant ROI

According to the Aberdeen Group's report, "Protecting Cardholder Data", organizations that have already implemented the necessary steps to achieve compliance are finding that the standard actually represents an excellent model for protecting all their critical data and systems. As such, they are seeing far greater potential return on investment (ROI) than they had originally expected.

A specific or quantitative ROI is difficult to describe in this paper. However, ROI from PCI is the product of the avoidance of penalties, the benefits gained through reduced risk of breaches, the opportunity to reduce the compliance costs of new or other regulations, and operational efficiencies through the investments in tools and processes.

Avoidance of Penalties

Clearly there is a direct return on the investment for organizations implementing PCI DSS resulting from the avoidance of penalties. Fines for non-compliance can reach as high as $100,000 per month, and organizations that are breached can have their credit card privileges revoked by the card companies[10]. VISA has already demonstrated the desire to enforce these measures, and in 2006, the credit card company levied $4.6 million in fines.[11] This represents a powerful incentive to most organizations to reach, maintain, and document their compliance.

Reduced Risk of Data Breaches

Forrester Research has estimated that the cost of a data breach ranges between $90 and $305 per record stolen, depending on how long it takes for the breach to be discovered. With records being stolen at a rate of 6 million per month, this represents a potential total liability of between $540,000,000 and $1.8 billion per month, or almost $22 billion per year.

When considering that the two most common and expensive forms of incident are fraud and insider attack, it is easy to see why businesses are now highly sensitive to the heightened level of exposure data theft carries. If, as many organizations now believe, PCI DSS represents one of the best current legislative approaches to securing data, then long-term and significant ROI can, and should, be realized from implementing its requirements.

[8] See ComputerWorld article, "Minnesota becomes first state to make core PCI requirement a law," at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9020923&intsrc=hm_list.

[9] See the 12th Annual CSI Survey on Computer Crime and Security (2007) found at http://www.gocsi.com/.

[10] For a good example of the potential penalties associated with a breach, read about the CardSystems Solutions breach at http://www.msnbc.msn.com/id/8629796/.

[11] http://www.news.com/Visa-takes-carrot-and-stick-approach-to-security/2100-1029_3-6143055.html

Quicker Response to New or Other Requirements

Early adopters of prior legislative requirements, such as HIPAA, SOX, Basel, etc., have typically found that there are significant common themes that run through them, especially in the areas of critical data protection, access control, and the systems that enforce them. While the specifics may vary, the approaches often share common objectives.

PCI DSS, as a standard specifically targeted to protect critical and sensitive data, should therefore provide organizations achieving compliance with an excellent starting point for any future, data-centric legislative efforts. Indeed, as the methodologies and approaches for securing data mature, it is likely that legislative efforts will both draw heavily on prior approaches, and that we will see increased convergence in standards. PCI DSS then, provides a good degree of “future-proofing” for implementers, and therefore helps provide good ROI over the lifetime of the organization.

Operational Efficiencies

In addition to specific gains related to compliance and security, there are other operational gains that result from more tightly integrated and streamlined security processes.

Operational incident management can be readily improved by providing easier and quicker access to log data, configuration information, and delta reports, which in turn facilitates root cause analysis speedier problem resolution.

Furthermore, by improving the operational integrity of systems with more effective change control and enforcement of baseline or standard configurations system availability and performance are inevitably enhanced. This provides further cost savings for both administration resources and end-user business processes. For example, NetIQ’s own Secure Configuration Manager can ensure systems are patched to the correct corporate standard, and are running appropriate systems management tools.

These operational efficiency gains can be more difficult to measure in the short-term, but over longer periods can become significant factors in reducing total IT expenditure, which itself frees resources for further operational streamlining.

How NetIQ Can Help

NetIQ is recognized as a world leader in the field of security event and information management, compliance, and policy management. While no single vendor can provide all the necessary tools to enable complete PCI DSS compliance, NetIQ’s unique breadth of knowledge and technology provides our customers with an excellent foundation upon which to build compliance programs.

NetIQ tools, solutions or security knowledge will enable more rapid compliance in all 12 areas defined by PCI DSS, either by directly securing information, systems and processes, or by enabling the better utilization of existing security technology.

In areas such as vulnerability detection, security event and log management, privilege management, and documenting all the processes involved, NetIQ’s tools can provide exceptional benefits to organizations not only seeking to reach compliance quickly but to continue to benefit from those efforts beyond the PCI deadlines.

Mapping NetIQ's products to PCI Objectives

Requirement	NetIQ			NetIQ Solution
1. Install and maintain a firewall configuration to protect data.		🔍	🔧	Security Manager
2. Do not use vendor supplied defaults for system passwords and other security parameters	🔒	🔍		Secure Configuration Manager, Security Solutions for iSeries
3. Protect Stored Data		🔍		Security Manager Security Solutions for iSeries
4. Encrypt transmissions of cardholder data and sensitive information on public networks			🔧	Security Manager, Secure Configuration Manager
5. Use and regularly update anti-virus software		🔍	🔧	Secure Configuration Manager
6. Develop and maintain secure systems and applications	🔒	🔍		Secure Configuration Manager
7. Restrict access to data by business need-to-know	🔒	🔍		Security Manager, Secure Configuration Manager, Change Guardian for Active Directory, Security Solutions for iSeries NetIQ Directory & Resource Administrator NetIQ Change Administrator for Windows
8. Assign a unique ID to each person with computer access	🔒	🔍		Secure Configuration Manager, Security Solutions for iSeries
9. Restrict physical access to cardholder data			🔧	Security Manager
10. Track and monitor all access to network resources and cardholder data	🔒	🔍		Secure Configuration Manager, Security Manager, Change Guardian for Active Directory, Change Guardian for Windows, Security Solutions for iSeries
11. Regularly test security systems and processes	🔒	🔍		Security Manager Security Solutions for iSeries
12. Maintain a policy that addresses information security	🔒			VigilEnt Policy Center, Security Manager

🔒 - Directly secure or enforce all or some of this policy or rule
🔍 - Directly monitor all or some of this policy or rule
🔧 - Support the enforcement of this rule through third-party applications
Platforms supported: Windows, Unix, IBM System i (iSeries), Linux.

Conclusion: Building on PCI for Better Security

Achieving PCI Compliance is not trivial. However, by following a well planned, well organized approach, organizations are certainly beginning to not only achieve it, but realized additional long-term benefits from their efforts.

Just as no single security solution can meet all your organization’s needs for securing your infrastructure and your data, so no single security vendor will be able to meet the entirety of your PCI DSS compliance needs.

However, having a vendor partner with a proven track record in the security and compliance space, offering solutions not only for the full range of PCI requirements but the majority of business platforms (Windows, Unix, Linux, IBM System i) can reduce your time to compliance and lower your costs.

NetIQ is such a vendor, and with customers in all sectors, both public and private, we have the experience and tools to help you attain your compliance goals more easily, more rapidly, and with less cost.

Finally, our long-term commitment to developing world-leading security management tools and to integrate them with operational management systems will ensure that any investment in PCI compliance generates significant security return on investment for the lifetime of your organization.

For more information on NetIQ’s PCI DSS compliance offerings, or our general security products, visit www.netiq.com.

Appendix A: Core Requirements for PCI DSS

The 12 general requirements for PCI DSS compliance are as follows[12]:

Build and maintain a Secure Network.

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other data

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

[12] See https://www.pcisecuritystandards.org/ for the full Payment Card Industry Data Security Standard document.

Appendix B: Complete Mapping of NetIQ Solutions

PCI Control Objective	Requirement	How NetIQ Can Help
Build & Maintain a Secure Network	1. Install and maintain a firewall configuration	• Publish firewall configuration policies on the intranet and track who has read them. • Monitor for changes or unauthorized access to Cisco-IOS based routers & switches.
	2. Do not use vendor-supplied defaults for passwords	• Check-up reports assess if systems are in compliance with password policies. • Pre-configured checks are automatically delivered when new vulnerabilities are discovered. • Tasks and actions can be used to disable insecure services. • Changes can be made to system configurations across multiple servers.
Protect Cardholder Data	3. Protect stored cardholder data	• Determine if proper security controls are in place to protect sensitive data. • Develop, distribute and enforce data retention and disposal policies.
	4. Encrypt transmission of cardholder data across open, public networks	• Safely transmit sensitive data and ensure transfers are complete. • Develop, distribute and enforce data cryptographic policies.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software	• Evaluate the status of anti-virus applications, including virus signature date, last scan date and scanning engine version. • Monitor anti-virus system services and restart.
	6. Develop and maintain secure systems and applications	• Audit to ensure the latest security patches are installed. • Provide automatic updates when new patches are released, and new vulnerabilities discovered. • Define entitlements for separation of duties. • Enable granular access control to reduce the number of privileged accounts. • Alert on unmanaged changes to Active Directory objects.

PCI Control Objective	Requirement	How NetIQ Can Help
Implement Strong Access Control Measures	7. Restrict access to cardholder data	• Delegate administrator rights to establish file and directory permissions. • Alert on failed administrator/user access and AD/Group Policy object changes. • Publish data control policies; track receipt and test understanding.
	8. Assign a unique ID to each person	• Report on user names across domains to ensure uniqueness. • Verify that user accounts are protected by strong passwords or smart card authentication. • Delegate administrative rights to set up user account properties. • Allow users to manage their own Windows passwords. • Report on user account activity, like last login.
	9. Restrict physical access to cardholder data	• Develop, distribute and enforce security policies on restricting physical access.
Regularly Monitor & Test Networks	10. Track and monitor all access to network resources and cardholder data	• Generate reports to verify auditing is enabled. • Analyze event logs in real-time, then archive for trending and forensics reporting. • Log and report on AD changes. • Monitoring actions taken by privileged users, as well as the creation/deletion of system objects.
	11. Regularly test security systems and processes	• Continuous monitoring of critical files and directories with alerting on changes. • Real-time notification of host-based threats and optional remediation.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security	• Built-in written security policies to define acceptable usage for IT assets and disaster recovery. • Real-time monitoring and alerting for security incidents. • Facilitates rapid incident response via workflow and knowledge base.

About NetIQ Corporation

A World Leader in Systems and Security Management

NetIQ delivers business-critical solutions to assure, analyze and optimize the performance, availability and security of your IT infrastructure.

Only NetIQ supplies the best-of-breed tools you need to Work Smarter—to manage and secure your critical infrastructure investments, such as servers, databases, web sites, email, voice and video and mission-critical applications. Not only can we help you customize and refine your Systems Management and Security Management controls to fit your particular environment, but we can also provide critical insights into your web site performance.

Focused on providing you with the competitive advantage necessary to survive and thrive in today's chaotic business environment, NetIQ offers a complete range of easy-to-deploy, cross-platform solutions—from our industry- and market-leading Windows Systems Management solutions to our solutions for Linux and UNIX; and from our integrated Security Management products to our award-winning WebTrends Web Analytics tools.

NetIQ counts more than 4,000 of the world's leading enterprises as key customers. In addition, our partnerships with industry leaders, such as Microsoft, IBM, HP and Dell, give NetIQ a unique advantage in the global marketplace. With customer-proven solutions and strong relationships, NetIQ delivers the tools you need to reduce your risk and deliver value from day one.

To learn more about NetIQ, visit us online at www.NetIQ.com.