

# Challenges and Opportunities of PCI

Sponsored by:

**TRIPWIRE**  
~~TRIPWIRE~~

# ComplianceINSIGHT

## Challenges and Opportunities of PCI

The control framework implicit in the Payment Card Industry Data Security Standard (PCI DSS) provides an enterprise structure for improving operational, security, and audit performance. The benefits of the PCI DSS go beyond audit costs and results, however. As a security model, PCI requirements can help companies control compliance costs and build a more efficient and reliable IT infrastructure that delivers better service while incurring less risk. Alignment of business and PCI goals ensures that internal security standards remain consistent with PCI requirements and that security policies remain relevant and enforced.

## About the IT Compliance Institute

The IT Compliance Institute (ITCi) strives to be a global authority on the role of technology in business governance and regulatory compliance. Through comprehensive education, research, and analysis related to emerging government statutes and affected business and technology practices, we help organizations overcome the challenges posed by today's regulatory environment and find new ways to turn compliance efforts into capital opportunities.

ITCi's primary goal is to be a useful and trusted resource for IT professionals seeking to help businesses meet privacy, security, financial accountability, and other regulatory requirements. Targeted at CIOs, CTOs, compliance managers, and information technology professionals, ITCi focuses on regional- and vertical-specific information that promotes awareness and propagates best practices within the IT community.

**For more information, please visit: [www.itcinstitute.com](http://www.itcinstitute.com)**

## Table of Contents

- 2** Identifying the Challenges of PCI
- 3** The Basics of PCI
- 4** Exploiting the Opportunities of PCI
- 5** The Payoffs of Control Frameworks
- 5** Improve Business Performance with PCI DSS Controls
- 6** Measuring PCI Performance Gains
- 7** Using PCI Mandates to Improve Business Operations
- 8** Suggestions for a Smooth PCI Implementation
- 10** Solutions for PCI: PCI-Mandated Monitoring and Change Control with Tripwire Solutions

All design elements, front matter, and content are copyright © 2007 IT Compliance Institute, a division of 1105 Media, Inc., unless otherwise noted. All rights are reserved for all copyright holders.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under § 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the copyright holder.

Limit of Liability/Disclaimer of Warranty: While the copyright holders, publishers, and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of its contents and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be usable for your situation. You should consult with a professional where appropriate. Neither the publishers nor authors shall be liable for any loss of profit or any other commercial damages, including, but not limited to, special, incidental, consequential, or other damages.

All trademarks cited herein are the property of their respective owners.

## Challenges and Opportunities of PCI

The greatest risk to credit card data is constantly evolving exploits that target both technical and administrative vulnerabilities in information systems. The Payment Card Industry Data Security Standard (PCI DSS) addresses those vulnerabilities, specifically those affecting sensitive cardholder data, and sets forth requirements companies must meet to minimize the impact of those vulnerabilities on security. The PCI standard requires continuous validation of security efforts, so companies complying with PCI DSS can't simply implement solutions and then forget about them.

Experience has shown that PCI DSS compliance is most successful when it's coordinated with corporate business processes. Integrating the DSS with corporate security standards ensures that security controls are rigorously enforced and remain consistent with PCI requirements. Such coordination also contributes to more cost-effective auditing, a stronger enterprise security profile, and a more streamlined and reliable IT infrastructure that can deliver better service while incurring less risk.

Implementing the PCI DSS also opens the door to improving business processes and enterprise information security operations. To recognize these opportunities and how to best take advantage of them, it's important to first appreciate the challenges posed by PCI compliance.

### Identifying the Challenges of PCI

Companies must first understand the requirements of PCI DSS to ensure proper implementation. This effort that can be daunting for those less experienced in putting security-related best practices to work. Also, before any work on PCI DSS implementation begins,

corporate decision makers must determine the organization's pre-audit PCI status.

Many managers considering PCI DSS implementation soon discover that they face several complex technological challenges; most notably:

- Tracking and monitoring access to the network and systems containing cardholder data
- Encrypting cardholder data
- Controlling logical access to systems with cardholder data
- Authenticating users who access systems containing cardholder data
- Detecting and preventing intrusion and scanning for vulnerabilities
- Penetration testing
- Installing and maintaining firewalls

PCI DSS auditors often discover myriad vulnerabilities, such as inconsistent encryption techniques across merchant systems and networks, storage of unnecessary cardholder data, transmission of cardholder data over unsecured networks, lack of regular vulnerability scanning and inadequate logging—or no logging at all—of network activity.

It's not unusual for companies to assume that, because they're already compliant with Sarbanes-Oxley or HIPAA requirements, they are also PCI-compliant. They soon discover that implemented controls<sup>1</sup> are insufficient to meet the PCI standard.

## THE BASICS OF PCI

### WHO IS AFFECTED

Covered entities comprise all Visa International, MasterCard Worldwide, Discover Financial Services, American Express, and JCB members, merchants, and service providers that store, process or transmit cardholder data. PCI regulates point-of-sale, telephone, online, and all other types of transactions.

### WHAT IT COVERS

All "system components" are covered. These are defined by the PCI DSS as "any network component, server, or application included in, or connected to the cardholder data environment."

### HOW IT'S ENFORCED

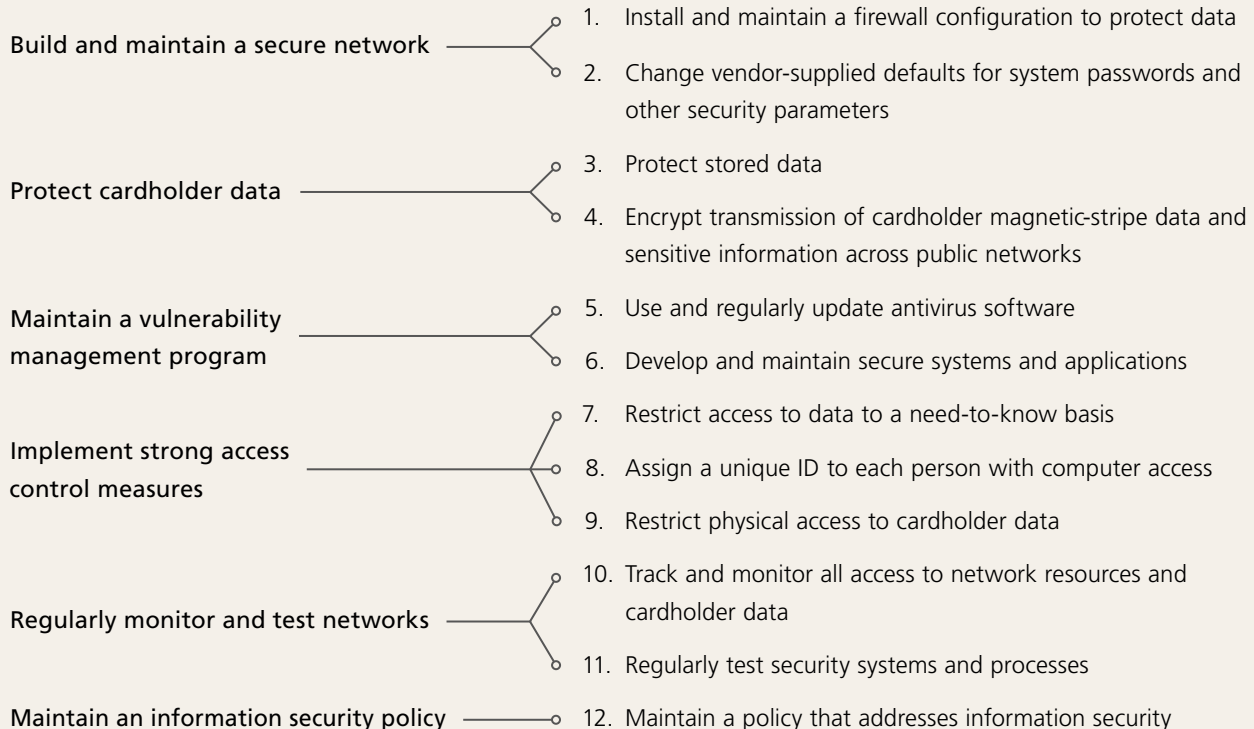
PCI is an industry-regulated security standard in most states, although Minnesota recently been implemented the standard into law in and several other states have proposed that it become law. Since state law generally supersedes industry requirements, the exact mechanism of enforcement in Minnesota, and potentially other states, remains a question of much interest and debate at the time of this writing. In states other than Minnesota, however, adherence to the PCI DSS is regulated by contracts between the sponsoring major credit card companies and their members, merchants, and service providers. PCI is enforced through:

- Contractual penalties and/or sanctions, including fines of up to \$500,000 per incident and revocation of a company's right to accept or process credit card transactions.
- Validation requirements to maintain and demonstrate compliance. These vary among payment card companies and depend on a merchant "level" tied to risk recognition and transaction or account volume. In their most comprehensive form, the requirements include onsite security audits, self-assessment questionnaires, mandatory penetration testing, and network scans.

## Twelve Steps to PCI Compliance\*

### CONTROL OBJECTIVES

### COMPLIANCE REQUIREMENTS



\* The Payment Card Industry Data Security Standard (PCI DSS) includes numerous sub-requirements not listed here. To see these, visit <http://www.pcisecuritystandards.org>.

## Exploiting the Opportunities of PCI

Security standards are certainly not new. During the Great Depression, for example, at least one county government in Midwestern America issued Springfield rifles to local shopkeepers so they could shoot at fleeing bank robbers (anecdotal evidence suggests that this practice reduced the crime rate in general).

The 21st century requires new security measures to defend against the new and emerging threats to which virtually all businesses are now vulnerable. Despite these challenges, implementing the PCI standard doesn't need to be yet another painful cost of doing business.

Fortunately, compliance with the PCI standard is a lot less dangerous than shooting at bank robbers. Compliance does provide a similar advantage, though: companies that implement PCI DSS protect their sensitive data, but also prepare their businesses to comply with future security standards that will undoubtedly evolve in response to emerging threats and vulnerabilities.

By getting ahead of the compliance curve, organizations that implement PCI DSS can actually reduce long-term compliance costs. Putting the robust PCI standard in place instills security best practices across the entire enterprise, making it easier and less expensive to adhere to new requirements down the road, and creating a leaner, more efficient organization.

Thought leaders in the areas of compliance and information security typically recommend that organizations undertake a systematic, comprehensive approach involving several steps. The first step is to articulate business requirements. This leads to the next step, developing a risk assessment that helps generate both security policy and control<sup>1</sup> frameworks. Finally, these frameworks form the basis for a technology architecture, including guidelines and control standards, and help form policy management and feedback processes.

Such a wide-ranging effort happens within the context of the relevant compliance mandates and their various

requirements. When a company has to meet multiple compliance mandates, it's faced with a new challenge—ensuring compliance with the fewest possible processes and tools.

Here is where broad-based control frameworks can help. The IT Governance Institute's Control Objectives for Information and related Technology (CobIT)<sup>2</sup>, International Organization for Standardization (ISO) 17799/27002, National Institute of Standards and Technology (NIST) 800-26, and Information Security Forum (ISF) standards and frameworks provide knowledge bases that serve as a template, or starting point, for companies creating compliant policies and assessing technical and non-technical controls.

---

**Fortunately, compliance with the PCI standard is a lot less dangerous than shooting at bank robbers.**

---

And because PCI is also an integrated framework, it also forms a foundation for a robust, company-wide IT security practice. The PCI standards that govern how merchants process, store and transmit cardholder data ultimately constitute a comprehensive integrated framework. This framework combines technology, policies, education, awareness and industry best practices.

An organization can generalize PCI requirements across its data, networks, systems, business processes, and transactions. What's more, implementing the kind of control framework implicit in the PCI DSS leads to measurable improvements in operational, security and audit performance.

---

<sup>1</sup>"Control" has a somewhat narrower meaning here. A control is a policy or procedure that prevents, detects, or corrects unlawful events.

<sup>2</sup> CobIT is most frequently used for Sarbanes-Oxley Act compliance, but can also be used to meet other mandates, such as the PCI DSS, and to ensure security and availability of IT assets in general.

## The Payoffs of Control Frameworks

In 2006, the IT Process Institute (<http://www.itpi.org>) completed a study on IT control performance.<sup>3</sup> The study shows how the use of controls—policies and procedures that prevent, detect or correct unlawful events—improves operational, security and audit performance. The study also demonstrates how some controls deliver more performance punch than others.

Based on an analysis of 63 CobiT control activities, 25 key operations, and security and audit performance measures, the study's authors identify 21 control activities. They label these foundational controls and find that these controls deliver “substantial” returns on investment by:

<sup>3</sup>IT Controls Performance Study, IT Process Institute (<http://www.itpi.org>), 2006.

## IMPROVE BUSINESS PERFORMANCE WITH PCI DSS CONTROLS

### ACCESS CONTROLS (PCI 1, PCI 3, PCI 4, PCI 7, PCI 8, PCI 9)

- › A formal process for requesting, establishing, and issuing user accounts
- › An automated means of mapping user accounts to an authorized user
- › Well-defined roles and responsibilities for IT personnel
- › Regular review of control violations and security logs activity to identify and resolve unauthorized access incidents

### CHANGE CONTROLS (PCI 1, PCI 5, PCI 6, PCI 10, PCI 11)

- › Tracking of the change success rate
- › Monitoring of systems for unauthorized changes
- › Defined consequences for intentional unauthorized changes
- › Use of change success rate information to avert potentially risky changes

### CONFIGURATION CONTROLS (PCI 2)

- › A formal process for IT configuration management
- › An automated process for configuration management
- › Communication of IT infrastructure configurations, including physical and functional specifications, to relevant personnel

### RELEASE CONTROLS (PCI 6)

- › A standardized process for building software releases
- › Maintenance of a release-testing environment identical to the production environment
- › A definitive software library (DSL)

### SERVICE LEVEL CONTROLS (PCI 12)

- › Regular review of the IT service catalog
- › A service improvement program
- › A formal process for defining service levels

### RESOLUTION CONTROLS (PCI 10)

- › Tracking of the percentage of incidents fixed on the first attempt (“first-fix rate”)
- › A knowledge database of known errors and problems
- › Prioritization of rebuilding, rather than repair, during an incident
- › A defined process for managing known errors

\* Measured in terms of operations, security, and audit performance.

Sources: IT Controls Performance Study, IT Process Institute (<http://www.itpi.org>), 2006; Payment Card Industry (PCI) Data Security Standard Version 1.1, September 2006 (<http://www.pcisecuritystandards.org>).

- Improving how companies use existing resources (people and assets)
- Reducing ongoing operating costs
- Better aligning IT with business needs
- Lowering audit, compliance, and security costs

According to the study, companies that implement more of the 21 foundational controls generate higher performance across “virtually all” of the 25 performance measures used in the study. In eight of those measures, the top implementers perform at such a higher level compared to the lowest-implementing firms, that the study notes the difference as “statistically significant at the 5 percent level.”

Of these eight performance measures, three are operational controls: user satisfaction, operations spending (IT and total), and weekly maintenance time. The other five are security controls that, when combined, comprise the difference between protecting the business and leaving it

exposed to the risks and costs associated with both malicious and accidental events. Those security controls cover:

- Security sufficiency
- Security operations integration
- Percent of security breaches automatically detected
- Percent of security breaches from internal sources
- Access detection speed

The study also identifies six release, service level, resolution, and access controls. These indicate that an organization is building its control systems and differentiate medium-performing companies from the low-performers. The relevant controls are:

- A standardized process for building software releases
- A formal process to define service levels

## MEASURING PCI PERFORMANCE GAINS

Results of the IT Process Institute’s 2006 IT Controls Performance Study indicate that when a security breach occurs, top performers fare significantly better than medium and low performers:

- **Loss from security events:** Top performers experience security-related loss 29 percent less frequently than medium performers, 84 percent less than low performers
- **Detection of security breaches via automated controls:** Top performers detect breaches 52 percent more frequently than medium performers, 581 percent more than low performers

Top performers also significantly outdo medium and low performers when it comes to operations:

- **Unplanned work:** Top performers incur 12 percent less unplanned work than medium performers, 37 percent lower than low performers
- **Changes success rate:** In top performers, changes are 11 percent more likely to be successful than in than medium performers, 25 percent better than in low performers
- **First-fix rate:** Initial fix attempts are 45 percent more likely to be successful in top performers than in medium performers, 56 percent more likely than in low performers
- **Servers per system administrator:** Top performers have 2.5 times more servers per system administrator than medium performers, 5.4 times more than low performers

Source: IT Controls Performance Study, IT Process Institute ([www.itpi.org](http://www.itpi.org)), 2006.

- A knowledge database of known errors and problems to resolve incidents
- IT personnel assignments to well-defined roles and responsibilities
- Regular review of violation and security activity logs to identify and resolve incidents of unauthorized access
- Tracking of the percentage of incidents fixed on the first attempt

Controls that deliver sustained and continuous improvement help avert high-risk activities and proactively stabilize the IT environment. These controls, which mostly concern change and configuration issues, differentiate top-performing companies from the medium-performing firms. The study identifies six such controls:

- Monitoring systems for unauthorized changes
- Defining consequences for intentional unauthorized changes
- Establishing a formal process for IT configuration management
- Automating configuration management processes
- Tracking the organization's change success rate
- Providing relevant personnel with correct and accurate information on current IT infrastructure configurations, including their physical and functional specifications

The IT Process Institute study shows how organizations that take the time and trouble to implement these key controls can spot security breaches more quickly and suffer significantly reduced losses resulting from security incidents. Commitment to implementing the right controls also contributes to a more efficient, more productive enterprise by reducing unplanned work related to security

threats, improving change management within development environments, increasing developers' ability to fix software problems the first time around, and reducing the staff resource costs of managing the server environment.

## Using PCI Mandates to Improve Business Operations

Most of the highest-performing foundational controls identified by the IT Process Institute are also PCI DSS mandates. Several PCI requirements that distinguish top-performing organizations include the types of change controls, continuous monitoring and validation, and automatic change detection. These controls include:

- *Installing and maintaining a firewall configuration to protect data (PCI requirement 1)*. This includes a formal process for approving and testing all external network connections and changes to the firewall configuration. The PCI DSS also demands other network information, including an up-to-date diagram of pertinent network connections, descriptions of network component management, and lists of services and ports.
- *Developing and maintaining secure systems and applications (PCI requirement 6)*. Adherence involves following change-control procedures for all system and software configuration. Controls include documenting change impact, testing operational functionality, and obtaining management sign-off.
- *Regularly testing security systems and processes (PCI requirement 11)*. The PCI standard requires file-monitoring software to perform critical file comparisons at least daily, and to alert personnel to unauthorized modifications of critical system or content files.

PCI DSS also addresses audit procedures in requirement 10, which covers tracking and monitoring access to

network resources and cardholder data. Relevant mandates include:

- Automating audit trails for all system components to reconstruct key events
- Recording key audit trail entries for all system components for key events
- Securing audit trails so they can't be altered
- Retaining audit trail history for at least one year

Like many security-oriented audit requirements that seem unreasonably burdensome at first, the PCI DSS rules can ultimately pay for themselves by averting costs associated with security breaches—especially undetected breaches that compromise large amounts of sensitive data over long periods of time<sup>4</sup>.

Other PCI requirements can yield additional benefits. These include:

**Encryption and hashing:** PCI 3.4 requires that credit card numbers are protected via encryption, hashing, truncation, or index tokens. Credit card encryption systems can also encrypt other kinds of sensitive data at minimal additional cost. Altering search algorithms to use hashed values, rather than real values, is an effective risk mitigation strategy that's easy to implement for other kinds of records.

**Vulnerability handling:** PCI 6.2 requires a process to identify new vulnerabilities in systems that handle cardholder data. Such processes can be expanded cost effectively to all systems where sensitive data resides, reducing the likelihood of systems succumbing to

---

<sup>4</sup> Consider the TJX data breach discovered in early 2007. Two months after discovering the breach, TJX admitted that the data for at least 45.7 million credit and debit cards was stolen by hackers. The hackers were able to penetrate the network over a period of at least 18 months. So far, the company reports, costs associated with the breach have reached \$17 million.

new vulnerabilities, improving the availability of business-critical systems, and reducing losses in revenue and productivity from unplanned downtime.

**Strong authentication:** PCI 8.1-8.5 requires a strong authentication strategy. Companies can implement strong authentication across all business-critical systems for a small incremental cost per system. The benefits? Significantly lowered likelihood of unauthorized access to systems and data as well as reduced costs related to unauthorized access..

---

Like many security-oriented audit requirements that seem unreasonably burdensome at first, the PCI DSS rules can ultimately pay for themselves by averting costs associated with security breaches.

---

**Incident response planning:** PCI 12.9 requires a comprehensive incident response plan. Developing and implementing such a plan for all potential incidents, rather than just those involving credit card transactions, prepares an organization for many situations and helps them resume normal operations more quickly with less revenue loss.

Implementing PCI DSS thus offers organizations three kinds of payoff:

- Better protection for sensitive data, the networks that transport it, and the systems on which it resides
- The ability to adapt to future compliance mandates quickly and easily
- A leaner, more efficient enterprise

## Suggestions for a Smooth PCI Implementation

Companies embarking on a PCI DSS implementation can benefit from the experience of those that have already done it. Here are some of their suggestions:

**Figure out what you need to do.** Begin with the *Payment Card Industry (PCI) Data Security Standard Version 1.1 and PCI DSS Security Audit Procedures*, issued by the PCI Security Standards Council (<http://www.pcisecuritystandards.org>). Since PCI auditors use these documents to assess compliance, the guidance is a critical resource in understanding and meeting PCI requirements.

**Create an enterprise-wide compliance program.** Addressing new compliance mandates one by one results in an overly complex and under-responsive control environment burdened by the costs of redundant tools and a fire-drill management mode. By taking a comprehensive approach to compliance based on reusable frameworks built on widely-accepted standards and best practices, companies can reduce compliance and security costs and improve operational performance in IT and business units.

**Get used to encrypting data.** PCI DSS requires that companies encrypt specific kinds of sensitive data during transmission “over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.” This includes wireless networks and cell phones.

**Segment servers and networks with cardholder data.** Companies should implement technologies such as firewalls and routers with access control lists (ACLs) to technically protect systems and networks. Physical security controls are also necessary to segregate server equipment. Focusing controls only on systems that store cardholder data can limit the scope and cost of a PCI audit.

**Retain only necessary data.** PCI DSS has strict rules to prevent unnecessary storage of some cardholder data (see PCI requirement 3). Payment transaction software should meet these requirements.

**Pay attention to change control.** Tools and solutions used for PCI compliance must have appropriate change control mechanisms that prevent unauthorized changes from threatening the integrity and stability of software and systems. Change monitoring should be automatic and should alert appropriate managers when violations occur.

**Be nice to the auditors—and be ready for them.** Approach a PCI compliance audit as a cooperative partner. Auditors make a distinction between compliance gaps that are not in place and compliance gaps that have a target date for completion, so it’s worthwhile to be able to demonstrate plans for remediation of weak control areas.

**Speak up.** The PCI Security Standards Council, which controls PCI DSS, listens to constituents in the payment card industry. Communicating with the Council and auditors if faced with compliance difficulties can help reveal viable compliance alternatives.



## PCI-mandated Monitoring and Change Control with Tripwire Solutions

Consumers, governmental regulatory agencies and financial networks alike are growing concerned about the potential of security breaches within merchant technology environments. Their concern is well warranted: when sensitive financial data is stolen, consumers can suffer significant financial loss and are forced to devote countless hours to restoring their financial standing.

Merchants incur enormous risk when they fail to adequately secure such data: ruined reputation, brand erosion, decreased customer loyalty, increased scrutiny and harsh financial consequences from regulatory agencies and financial networks.

Because the risks are so great, businesses that accept major credit cards, like Visa and MasterCard, face special compliance mandates articulated in the PCI Data Security Standard. These mandates cover the storage, processing and transmission of cardholder data.

Tripwire can help organizations comply with PCI requirements in the area of file integrity monitoring, firewall and router security compliance monitoring and change control.

### Know your changes

Even if a company's IT infrastructure is in perfect PCI compliance, just one small change to a server or network device can be disastrous if that change isn't properly detected and reported. IT teams have few options for minimizing damage when changes aren't reported or if they don't know whether or not those changes are authorized. By exposing unauthorized or unintended changes, Tripwire can help validate internal processes.

Tripwire solutions monitor critical files and alert appropriate personnel to any unauthorized changes. These reporting capabilities give PCI auditors the information they need to complete quarterly and annual testing and reporting audits. Not only is this insurance against the financial impact of fines, it also provides the time and resources needed to prepare for audits.

### Change auditing matters

Tripwire's automatic change detection and configuration validation can save IT teams hours of valuable time every day. Without Tripwire change auditing, something as simple as a configuration mismatch or missed server can lead to hours of troubleshooting, often ending with costly manual intervention to determine the exact problem.

To validate PCI compliance, organizations should combine technical measures, administrative best practices and sound IT decision-making into an organized program of change auditing. By ensuring that PCI DSS requirements are in place, that reliable records exist to support compliance during validation and that any changes can be tracked and demonstrated, organizations subject to PCI compliance can be where they want to be when audit time rolls around.

### For more information:

[www.tripwire.com](http://www.tripwire.com)

US TOLL FREE: 1.800.TRIPWIRE

MAIN: 503.276.7500

FAX: 503.223.0182

326 SW Broadway, 3rd Floor

Portland, OR 97205 USA