

# Organizations See PCI as a Benefit, Not a Burden



White Paper

## Top 10 Takeaways from the Cisco PCI Survey

1. Most organizations have taken significant steps to achieve PCI compliance and believe their current infrastructures would pass assessments.
2. Organizations believe they are more secure than they would be if PCI compliance were not required.
3. Companies view PCI compliance as necessary for protecting cardholder data.
4. PCI compliance projects can drive or fund other network and information security projects.
5. Most organizations plan to increase PCI compliance spending in 2011.
6. Many companies plan to make additional investments to comply with evolving PCI requirements for virtualized environments.
7. Nearly two thirds of organizations are using point-to-point encryption, which will reduce the scope of PCI assessments and simplify compliance.
8. Most large and midsize organizations now use continuous wireless intrusion prevention and intrusion detection to guard against rogue wireless access points.
9. Other regulations, laws, and standards can enhance a company's ability to comply with PCI standards.
10. Educating employees on the proper handling of cardholder data remains the biggest challenge organizations face.

## Cisco Survey Reveals Changing Views on Compliance with the Payment Card Industry Data Security Standard

### What You Will Learn

Cisco recently commissioned a survey of 500 IT decision makers to gauge opinions about their efforts to comply with the Payment Card Industry Data Security Standard (PCI DSS). The survey revealed the following:

- Most organizations are now complying with the PCI standard.
- Opinions about PCI compliance are largely positive, across all industries.
- Companies are aware of and prepared for the latest version of the PCI standard.
- Organizations are investing significant resources in PCI compliance.
- Educating employees remains the most challenging aspect of PCI compliance.

### Introduction

Since the PCI DSS was first introduced in 2005, it has provoked its share of controversy. Especially in the first few years of implementation, as organizations tried to understand and adjust to new payment processing and data storage requirements, many companies—and even some major industry groups—expressed a sense that PCI DSS compliance was overly expensive and burdensome. Some also questioned whether the standard was necessary or even effective.

Cisco is pleased to report that such sentiments are no longer the norm. Cisco recently completed a survey of 500 IT decision makers involved in PCI compliance. Respondents represented a broad range of businesses, from small companies to large enterprises across multiple industries. In spite of this diversity, the survey returned one overwhelming message: Organizations of all types view PCI compliance as a necessary and worthwhile investment.

Among other results, the survey revealed the following:

- 85 percent of respondents are comfortable with their existing infrastructures in terms of PCI compliance and believe they would pass an assessment.
- 70 percent of respondents feel their organizations are more secure than they would be if PCI compliance were not required.
- 87 percent of respondents feel that PCI compliance is necessary.

“These results should come as no surprise given the rising publicity and costs associated with data breaches and identity theft,” says John N. Stewart, Cisco vice president and chief security officer. “Going the extra mile to protect cardholder data makes sound business sense, in addition to just being the right thing to do. For many companies, PCI certification has become a market differentiator.”

Let’s explore the results of the Cisco® PCI Survey in greater detail.

## Profile of Respondents

The Cisco PCI Survey was conducted by research firm InsightExpress in November 2010. The results reflect the opinions of 500 IT decision makers, more than half of whom are the primary decision makers for their organizations’ PCI compliance efforts. The organizations ranged in size from small companies with 100 users up to large enterprises with thousands of employees, representing 100 businesses in each of five industries: education, financial services, government, healthcare, and retail.

Most of those surveyed (71 percent) report that they have been processing, storing, or transmitting credit card information for four years or longer—and therefore have been required to comply with PCI DSS since the standard was introduced.

Respondents resource their compliance efforts in a variety of ways, using in-house staff, outsourced PCI consultants, or a combination of the two. (Few respondents across all industries use contractors.) A clear majority of organizations surveyed (70 percent) handle at least some aspects of PCI compliance internally, suggesting that most companies now view PCI as important enough to warrant investment in in-house training and expertise.

## General Opinions of PCI

Given early complaints about the burden involved in complying with the PCI standard, some industry observers have assumed that many organizations are not yet fully compliant. In fact, the Cisco survey suggests the opposite: 85 percent

of respondents replied that they not only are comfortable with their existing network infrastructure, but also believe they would likely pass an assessment at the present time.

This high level of confidence spans all vertical industries surveyed. Not surprisingly, however, given the central role of payment cards in their businesses, retail and financial services organizations reported the most confidence in their present PCI compliance efforts. In both sectors, 92 percent of respondents believe they would pass a PCI assessment today. The fact that respondents from retail felt as comfortable in their likelihood of passing an assessment as financial services respondents indicates that this industry has made great strides in adoption and implementation efforts.

Among respondents in all industries who have undergone assessments, 78 percent passed, and another 16 percent passed contingent upon taking further action outlined in their assessment results. Perhaps surprisingly, government respondents fared better than all other sectors analyzed, with 85 percent passing their initial assessment. Healthcare organizations, unfortunately, fared the worst, with a 72 percent pass rate at the time of assessment.

In addition to these encouraging compliance results, the survey also indicates that, perhaps contrary to expectations, attitudes about PCI DSS among IT professionals are now quite positive. Overall, 70 percent of respondents report that their organization is more secure as a result of complying with the PCI standard. Among financial services and retail companies in particular, 78 percent believe that PCI compliance has improved overall security. In fact, half of retailers surveyed believe that their organizations are now much more secure as a result of PCI.

A slim majority (51 percent) of respondents feel that PCI compliance is burdensome, but most (87 percent) also believe that it is necessary. That sentiment is highest in healthcare and retail companies, where 90 and 92 percent of respondents, respectively, say that the standard provides necessary security precautions. Across all industries, very few respondents (5 percent overall) believe that PCI DSS does not go far enough to protect cardholder data.

## PCI DSS 2.0 and Virtualization

PCI DSS 2.0 was introduced in 2010 to provide additional guidance for complying with the PCI standard. According to the Cisco survey, organizations now view PCI as an important enough issue that most IT decision makers stay up to date on the subject. Among those surveyed, just 14 percent overall were unaware of the clarifications and recommendations in PCI DSS 2.0. Awareness was highest among financial services companies, with 94 percent of respondents in that industry reporting that they were at least somewhat familiar with the details of the new version of the standard. Awareness was lowest among government organizations, with 23 percent of respondents reporting that they were not aware of the PCI DSS 2.0 recommendations and clarifications.

One area that PCI DSS 2.0 was designed to address is virtualization, with the goal of clarifying the specific requirements for virtualized environments. The new standard classifies virtual environments as “system components,” leaving no doubt that they must be secured. Given that PCI DSS 2.0 specifically addresses this issue, one might assume that many companies’ virtual environments are not currently in compliance with the standard. The Cisco survey revealed, however, that 95 percent of respondents are either completely satisfied or somewhat satisfied with their current virtualization security postures. Once again, financial services companies are leading all industries in compliance, with 70 percent of respondents in that industry reporting that they are satisfied with their current posture.

However, respondents also identified virtualization as an area that will likely require additional investment to assure PCI compliance in the future. More than a third of all respondents (36 percent) anticipate needing to increase their number of virtual security appliances (such as firewall and intrusion prevention system [IPS] solutions) to comply with PCI DSS 2.0. Thirty percent plan to further harden their virtualization software using vendor-supplied guides and PCI guidance. Twenty-one percent report that they do not trust the hypervisor as a segmentation method for PCI, and thus anticipate needing to increase the number of servers they use.

“Although DSS 2.0 provides some important clarification on requirements for virtualized environments, there is still much to be decided in this rapidly evolving technology space,” says Stewart. “In the interim, organizations should ensure they are complying with the requirement that only one primary function is permitted per virtual system component or device. IT leaders should keep a close eye on virtualization in their cardholder data environments and establish program development and change control tollgates and processes to enforce this requirement.”

## Spending on and Investment in PCI Compliance

Organizations across all industries are making significant investments in their PCI compliance efforts, including PCI assessments. Most respondents (67 percent) believe their spending on PCI compliance will increase in the next year. Increases in PCI spending were anticipated in the financial services industry (75 percent of respondents) and retail (71 percent of respondents) in particular.

One of the most interesting and surprising elements of the survey involves the role of technology in payment environments. The PCI Security Standards Council has delivered only preliminary guidance on technologies not specifically included in the DSS, including the Europay, MasterCard, and VISA (EMV) standard for authenticating card transactions (commonly referred to as Chip and PIN) and point-to-point encryption (P2PE). Definitive standards, however, do not yet exist. And yet organizations seem to be adopting these technologies in the hope of reducing the scope of their card data environment that is subject to assessment.

Nearly half of those surveyed (45 percent) are using EMV to reduce the likelihood of fraud in transactions where cards are present. Another 23 percent were not yet using EMV but were thinking about it.

A whopping 60 percent of respondents use P2PE to simplify their compliance efforts and potentially reduce the scope of their next PCI assessment, and another 11 percent report that

they are thinking about using P2PE for those reasons. Nearly 70 percent of financial services organizations use P2PE. All of this suggests that, even in an environment where standards are not fully developed, organizations are not waiting to take action to address compliance, and are doing everything in their power to assure that card data and transactions are as secure as possible.

“It should come as no surprise that point-to-point encryption technologies are being deployed so widely as an aid to PCI compliance,” says Stewart. “If implemented correctly, those system components that simply pass through encrypted data and are segmented from the encryption and decryption environments can be excluded from the PCI compliance scope. We expect end-to-end encryption technologies to continue to play a major role in PCI compliance efforts.”

Of course, organizations use P2PE technology for a variety of reasons in addition to PCI compliance. But this response highlights another trend revealed in the PCI survey: A majority of IT decision makers (60 percent) are using PCI compliance projects to help fund other network security projects. Among financial services companies in particular, 72 percent of respondents report undertaking network security initiatives that have been at least partially funded or driven by PCI compliance.

“PCI requirements like log management and security incident monitoring can require significant up-front investment in tools and operational support,” says Stewart. “However, many companies are finding that, once these measures are established, augmenting information security in areas beyond the scope of PCI compliance can come at a relatively nominal cost.”

Another significant area of PCI-related investment has been continuous wireless intrusion prevention and intrusion detection (IPS/IDS) solutions, with a significant majority of respondents (58 percent) now using such solutions to police against rogue wireless access points. While some companies continue to use hand scanners for this purpose, for medium and large organizations, IPS/IDS has effectively become industry best practice.

## PCI Compliance Challenges

One concern among industry thought leaders is that the proliferating number of data security standards and compliance requirements will become confusing for businesses, or potentially even contradict each other. Fortunately, this does not appear to be the case. Eighty-five percent of respondents report that the various regulatory standards they follow are supportive of each other, at least in some measure. Forty-three percent (led by respondents in education organizations) say that complying with other regulations and standards has actually enhanced their ability to be PCI-compliant.

Respondents did report some challenges in their PCI DSS compliance efforts. The biggest issue: educating employees on the proper handling of cardholder data. Forty-three percent of respondents are experiencing this problem, and 27 percent rank it as the number one problem with which they contend in their PCI compliance efforts. Other problems identified by a significant number of respondents include having to upgrade antiquated systems to bring them into compliance (32 percent) and having to change business practices to comply with requirements (29 percent).

“As with most security issues, changing human behavior around card data is a more complex challenge than instituting the proper technologies,” says Stewart. “Companies should have PCI compliance training and awareness programs and supporting policy that communicates to employees the expectations for mandatory training and how it will be enforced. IT leaders should also maintain a current list of all users with access to cardholder data to ensure that those users are included in the training population. But training alone is not enough. Organizations also should put in place mechanisms to monitor and measure the effectiveness of that training.”

The survey asked respondents to identify the three requirements among the 12 PCI DSS requirements that caused them the most issues in achieving or maintaining compliance. Overall, respondents ranked the 12 requirements fairly evenly; there

was no single requirement that a majority identified as being significantly more problematic than all others. The requirement cited most often (ranked by 37 percent of respondents as a top concern) was tracking and monitoring all access to network resources and cardholder data.

The survey revealed some differentiation among different industries in the perceived challenge associated with these requirements. Among retail companies, for example, respondents identified protecting stored cardholder data as the biggest challenge. Among government and education organizations, respondents identified developing and maintaining secure systems and applications as the most challenging. In healthcare, respondents viewed tracking and monitoring all access to network resources and cardholder data as being the most problematic.

## Conclusion

However IT decision makers may have felt in the past about the PCI standard, they have clearly become fully engaged in bringing their organizations into compliance. According to the Cisco survey, these efforts are not merely the result of internal or industry mandates. A large majority of IT professionals now believe that PCI compliance not only is necessary, but that it makes their businesses more secure.

These sentiments are reflected in the growing investment in PCI compliance projects across all industries. Ultimately, these trends suggest a “win-win,” both for companies that process payment cards and for their customers. For consumers, industrywide compliance helps bolster confidence that their private financial information is secure. For businesses, higher levels of PCI compliance can translate into increased funding for other network security projects and, ultimately, allow for greater flexibility and security when transacting business with customers.

“This survey demonstrates that the PCI council is being successful in communicating and getting the active participation and increased adoption of the PCI standards among stakeholders. The findings also suggest that organizations are increasingly aware of the benefits of compliance. However, there continue to be challenges that need to be addressed in order to effectively protect cardholder data. Progress has been good, but there is much work still to be done,” says Fred Kost, director of security solutions, Cisco.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).