



2011 PCI DSS Compliance Trends Study

Survey of IT & IT security practitioners in the U.S.

Sponsored by Imperva

Independently conducted by Ponemon Institute^{LLC}

Publication Date: April 2011

2011 PCI DSS Compliance Trends Study

Survey of IT & IT Security Practitioners in the United States

Ponemon Institute, April 2011

Part 1. Introduction

The Payment Card Industry Data Security Standard (PCI DSS) continues to be one of the most important regulations for all organizations that hold, process or exchange cardholder information. In 2009, Ponemon Institute, with sponsorship from Imperva, conducted the first study¹ to determine if IT and IT security practitioners believe PCI compliance improves organizational security and how it affects the ability to respond to security threats affecting payment account data.

In this study, *2011 PCI DSS Compliance Trends Study*, we continue to examine how efforts to comply with PCI affects the organization's strategy, tactics and approach to achieving enterprise data protection and security and how the state of PCI compliance has changed since the first study. We also consider the reactions of IT and IT security practitioners in different-sized organizations have about compliance with PCI.

A key finding from this research is that there is a dramatic difference in the number of data breaches experienced by organizations considered compliant with PCI DSS and those that are not compliant. This is true for both cardholder data related incidents and general incidents. In fact, virtually all (99 percent) compliant organizations in this study report that they have had only one or no data breaches involving credit card data compared to 85 percent of non-compliant organizations that had one or no such breach incidents.

According to the majority of respondents, PCI-DSS compliance is primarily considered valuable in strengthening relationships with key business partners and helping to secure more funding for IT security. It is less likely to be viewed as enhancing brand or reputation in the marketplace. Approximately one-third (33 percent) of respondents in this year's study say PCI compliance contributes more value than the expenditures made. An almost equal percentage (32 percent) of respondents say PCI compliance contributes less value than what the organization invests.

A total of 670 US and multinational IT and IT security practitioners who are involved in their companies' PCI compliance efforts were surveyed on the following topics:

- What is the state of PCI DSS compliance in the organization?
- Who is most responsible in an organization for ensuring compliance with PCI DSS requirements?
- What technologies are preferred to achieve compliance with PCI DSS requirements?
- Does PCI DSS contribute to a decline in data breaches?
- Where are the greatest threats to the security of cardholder data located?
- What is the value PCI DSS compliance provides to the organization?

In this study, we closely examined the relationship of respondents' state of mind regarding PCI DSS to such variables as the level of compliance achieved in the organization and who leads the compliance effort. The more favorable the perception about PCI compliance the higher the level of compliance and the more likely the organization is to have responsibility assigned to the business unit or the CIO.

¹ See *2009 PCI DSS Compliance Study*, Ponemon Institute: September 2009

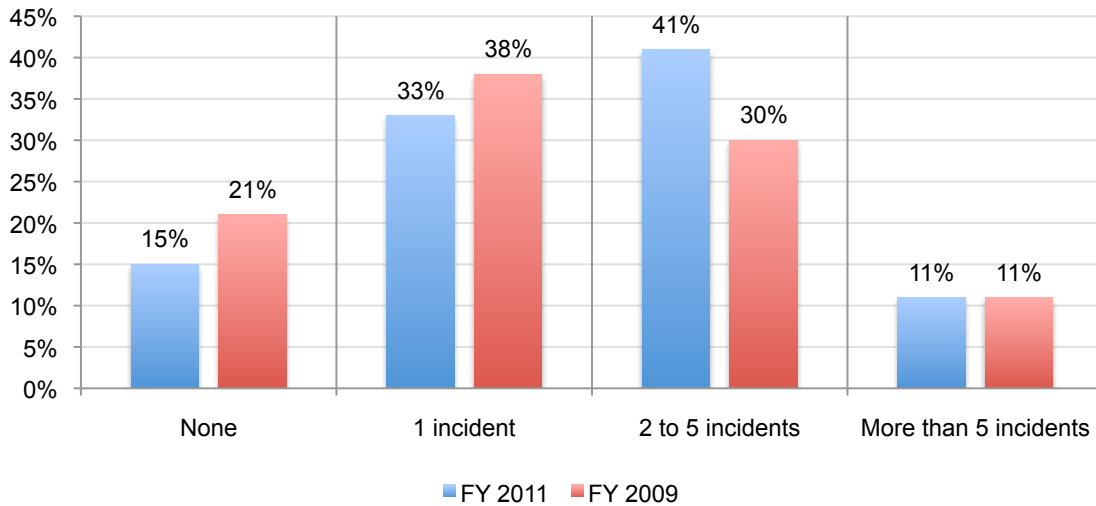
Part 2. Key findings

The percentage of data breaches reported increased from the 2009 study. However, organizations that are PCI compliant have fewer data breaches than non-compliant firms.

As shown in Bar Chart 1, the percentage of respondents reporting that their organization had a data breach in the past 24 months increased from 79 percent in 2009 to 85 percent in 2011. The largest increase concerns companies that reported two to five incidents over the past 24 months.

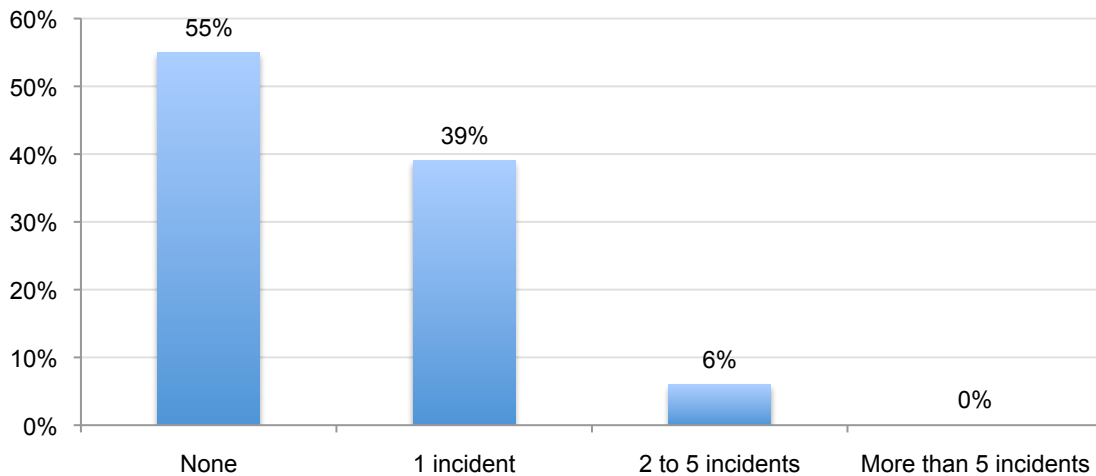
Bar Chart 1: Data breach experience in 2009 and 2011 studies (24 month period)

This series defines all data breach incidents including those involving cardholder data



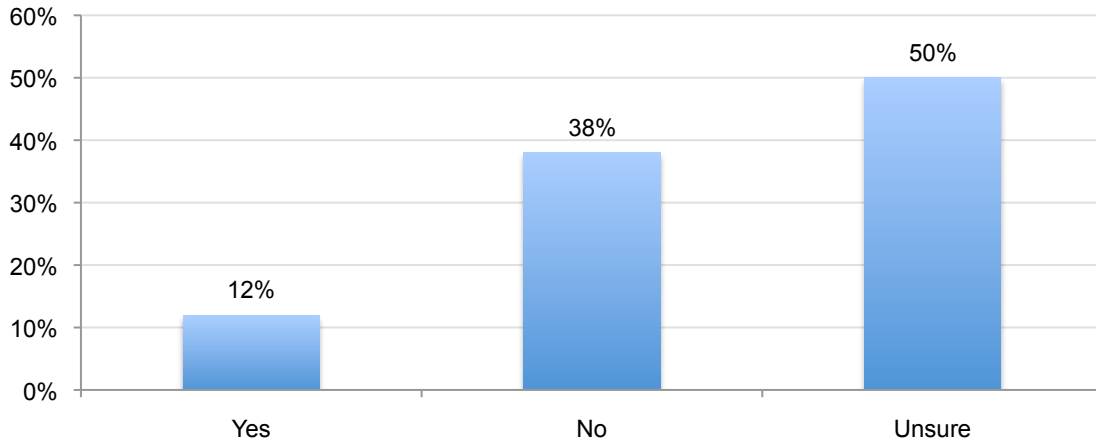
Bar Chart 2 shows that 55 percent of respondents say their organization's data breach incident did not concern the loss or theft of cardholder data. Thirty-nine percent say one of the data breach incidents involved cardholder data. Finally, six percent report two to five incidents involving cardholder data.

Bar Chart 2: Data breach incidents involving cardholder data over the past 24 months



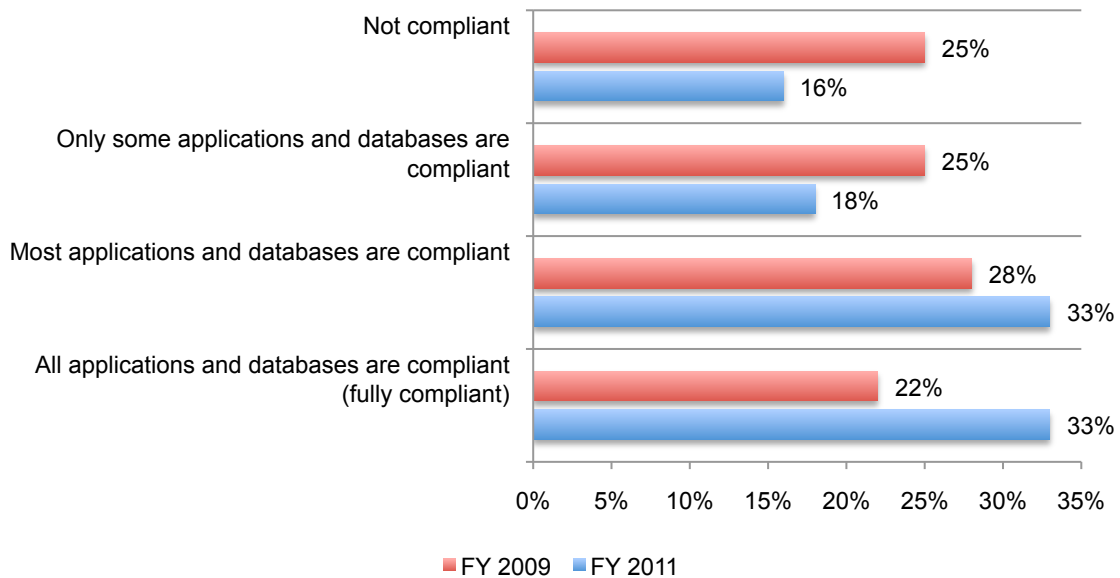
Bar Chart 3 shows 38 percent of respondents do not believe that PCI DSS resulted in a decline of data breach incidents. Another 50 percent of respondents are unsure about the impact of PCI DSS compliance on data breach. Only 12 percent believe PCI DSS compliance reduced data loss or theft.

Bar Chart 3: Perceived impact of PCI DSS on data breach experience



Bar Chart 4 reports the PCI compliance experience of respondents' companies in the 2011 and 2009 studies.² As can be seen, the percentage of non-compliant companies decreased from 25 percent to 16 percent. Correspondingly, the percentage of fully compliant companies increased from 22 percent to 33 percent.

Bar Chart 4: PCI compliance experience in 2009 and 2011 studies

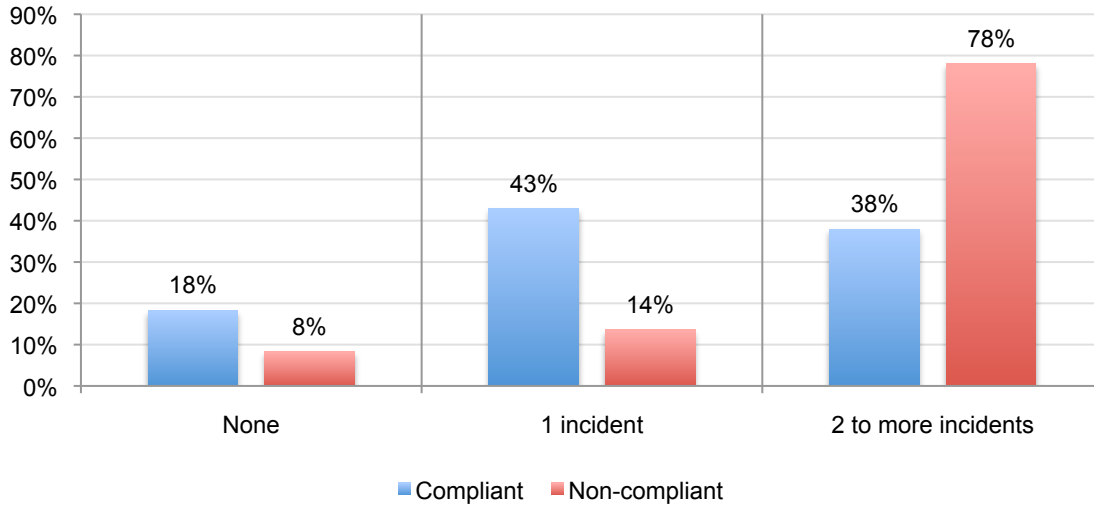


²For cross-tabulation purposes, we divided our sample based on responses to Q5 in the survey instrument. In total, 442 respondents (66 percent) were deemed to be PCI compliant if they chose "all" or "most applications and databases are compliant." The remaining 228 respondents (34 percent) were classified as PCI non-compliant if they chose "not compliant" or "only some applications and databases are compliant."

In our analysis, we looked at differences in data breach experience between organizations that achieved a high-level of PCI DSS compliance and those organizations that did not achieve a high-level of PCI compliance. What we learned from this cross-tabulation analysis is that 38 percent of the compliant organizations say their organizations had two or more breaches in the past 24 months versus 78 percent of respondents in the non-compliant group. These results are summarized in Bar Chart 5.

Bar Chart 5: Data breach experience for compliant and non-compliant groups

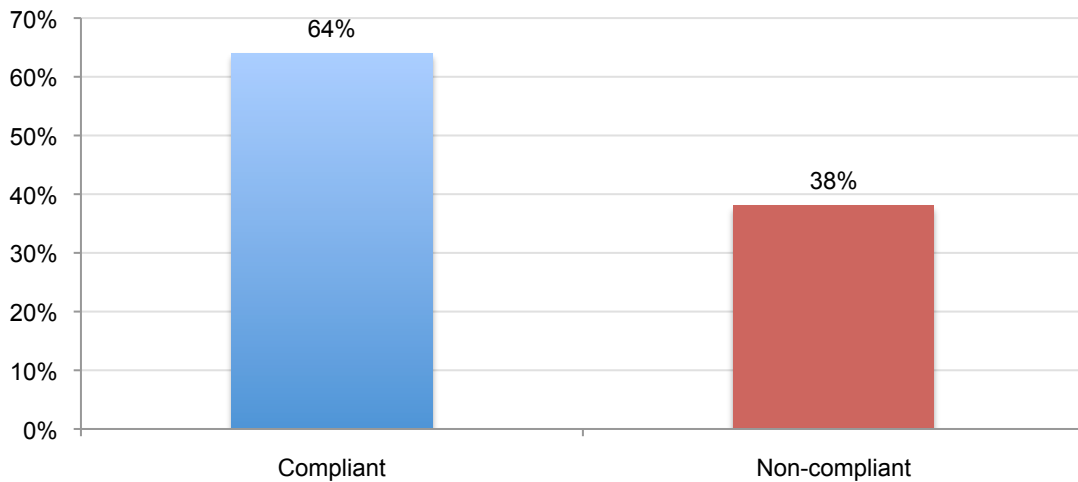
This series defines all data breach incidents including those involving cardholder data



Bar Chart 6 reports the percentages of compliant and non-compliant respondents who reported that their organizations did not experience the loss or theft of cardholder data during the past 24 months. Sixty-four percent of the compliant group did not have any breaches affecting cardholder data, while 38 percent of the non-compliant group says their companies did not have such a breach.

Bar Chart 6: Data breach of cardholder data for compliant and non-compliant groups

Each bar defines the percentage of companies that did not experience a breach over the past 24 months



Organizations that do not store primary account numbers (PAN) are less likely to experience the loss or theft of cardholder data.

Pie Chart 1 shows 66 percent of respondents say their organizations retain and store primary account numbers for various reasons. Table 1 lists these, which include customer services (52 percent), card reuse (49 percent) and charge backs (45 percent). Only 19 percent of respondents say their organizations use PAN for marketing analytics.

Pie Chart 1
Does your organization retain and store PAN (primary account numbers)

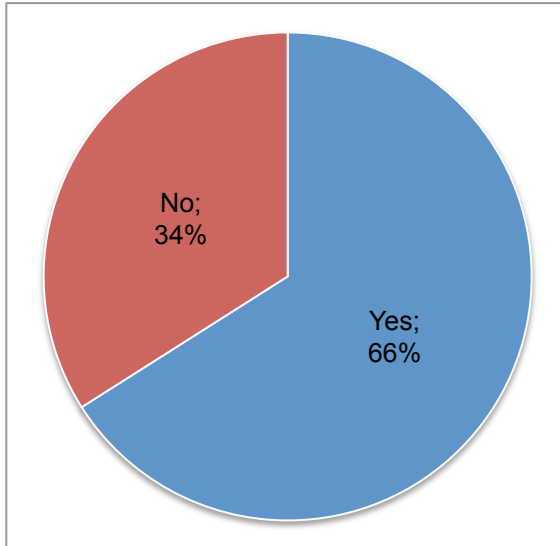
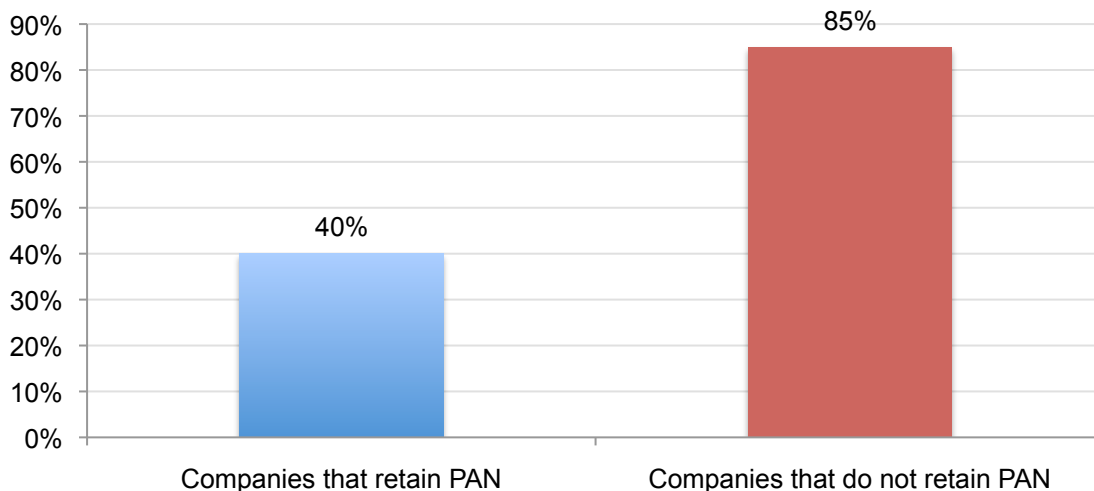


Table 1
Why does your organization retain and store PAN? Top two reasons.

Check all that apply	Pct%
Customer service	52%
Card reuse	49%
Charge backs	45%
Recurring subscriptions	31%
Marketing analytics	19%
Other	3%

Of the respondents who say their companies do not retain and store PAN, 85 percent did not experience cardholder data loss or theft over the past 24 months. In sharp contrast, only 40 percent of companies that retain and store PAN did not experience a breach involving cardholder data. These results are shown in Bar Chart 7.

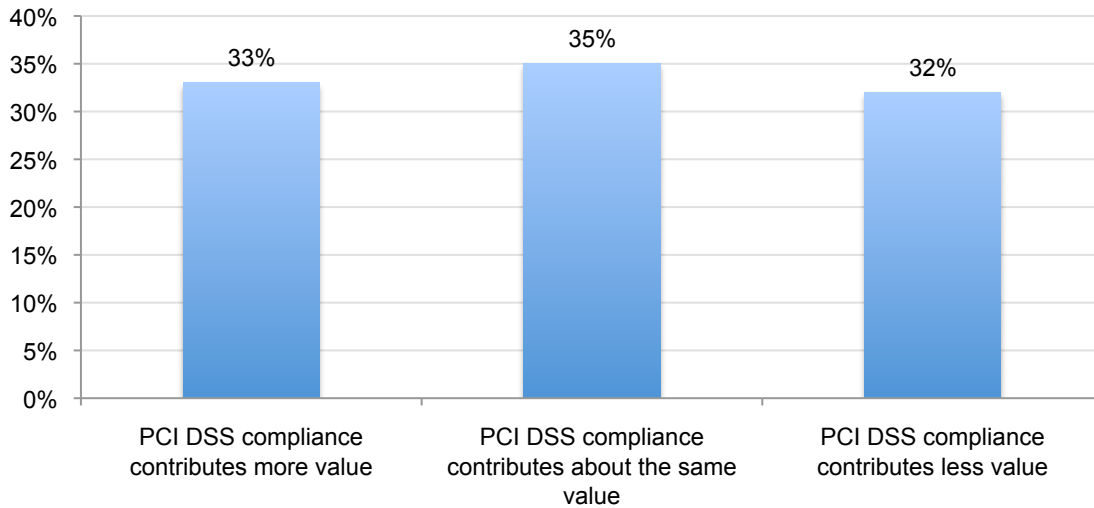
Bar Chart 7: Percentage of respondents' companies that did not experience a data breach involving cardholder data.



PCI DSS contributes about the same or more value than other security expenditures made.

Bar Chart 8 shows that one-third of respondents see PCI DSS compliance costs as adding more value than other IT security expenditures. Another 35 percent say these expenditures are at about the same level of value. Finally, 32 percent see PCI DSS compliance costs as adding less value than other IT security expenditures made.

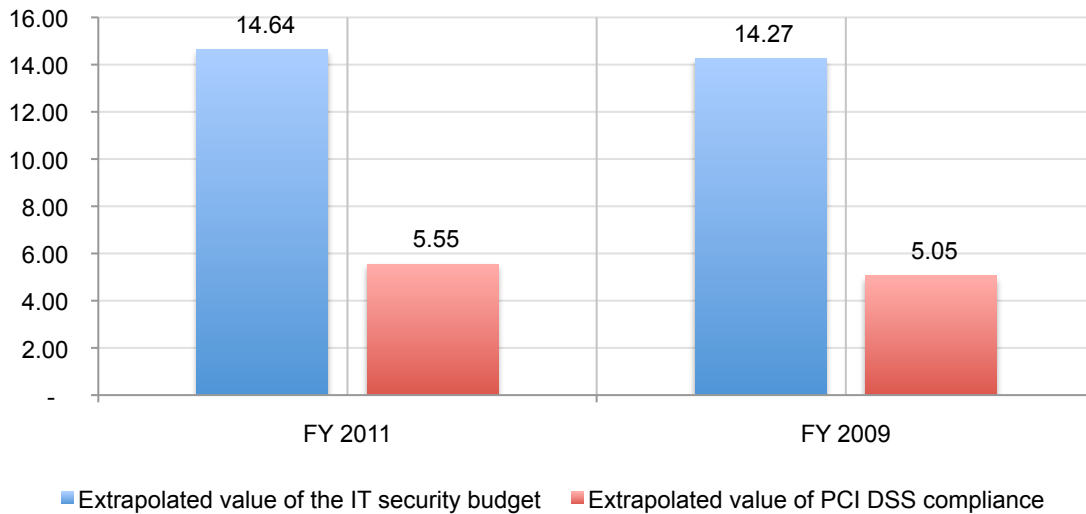
Bar Chart 8: Relative value of PCI DSS compliance expenditures



Bar Chart 9 provides the extrapolated average value that respondents' companies spend on IT security (total annual budget in FY 2011 at \$14.64 million versus \$14.27 million in FY 2009). This chart also shows the extrapolated average value for PCI DSS compliance expenditures. According to respondents, in FY 2011 companies are spending approximately \$5.55 million (or 38 percent) of their IT security budgets on PCI DSS compliance activities. This represents a small increase from our FY 2009 results.

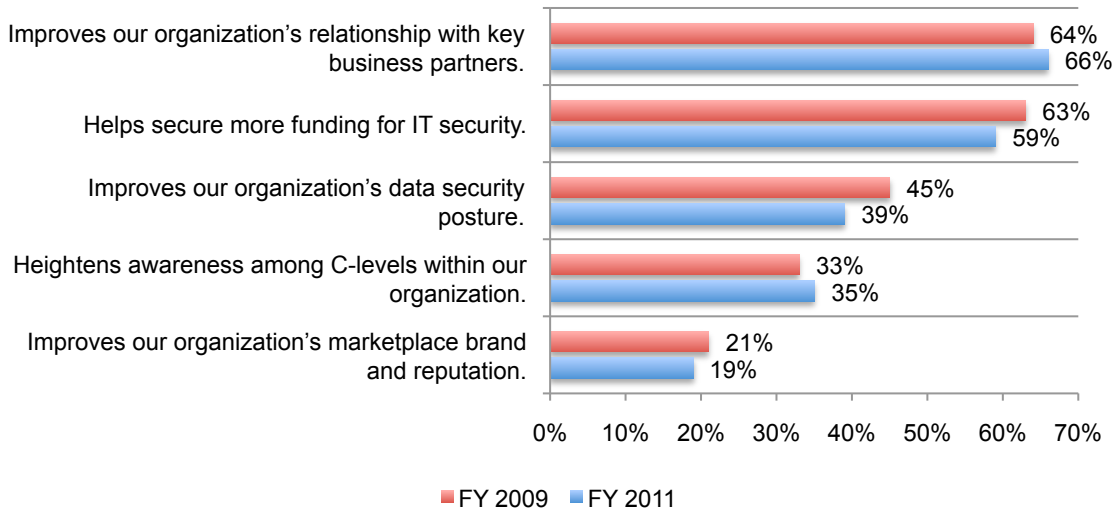
Bar Chart 9: Extrapolated average spending on IT security and PCI DSS compliance

\$1,000,000 omitted



Bar Chart 10 lists the perceived value propositions of PCI DSS compliance in both our 2011 and 2009 studies. According to respondents, the value proposition deemed most important concerns relationships with key business partners. The second most important value proposition is helping to secure more funding for IT security. The third most important value proposition is the improvement of the organization's security posture.

Bar Chart 10: Five value propositions for PCI DSS compliance

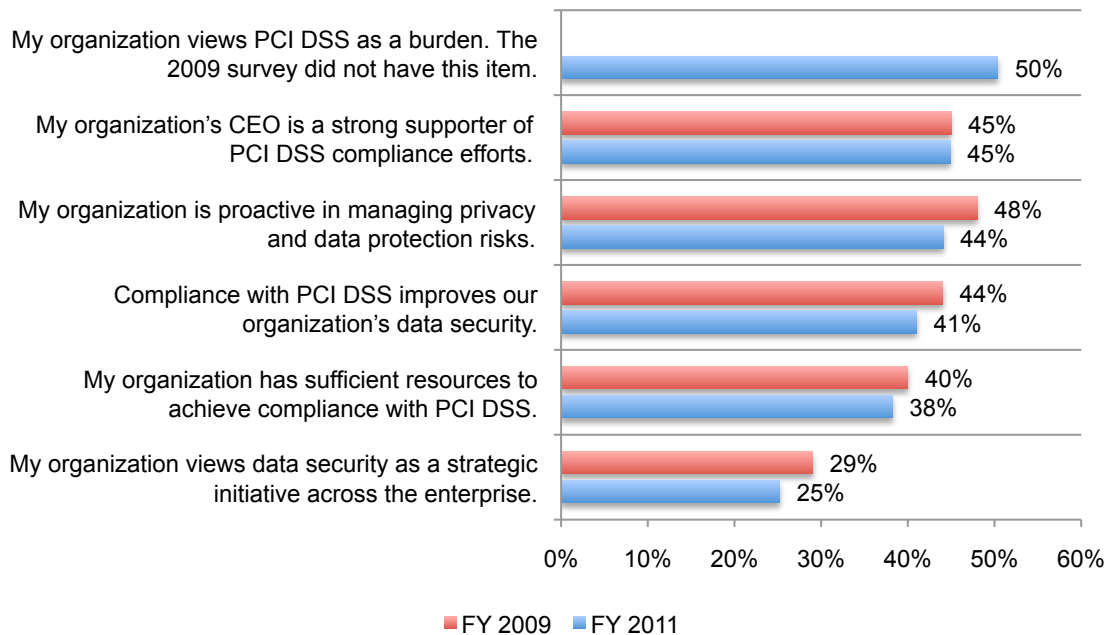


Organizations with a favorable perception about compliance with PCI DSS generally have achieved compliance across the enterprise and have fewer data breach incidents.

The following bar chart summarizes the strongly agree and agree response to six statements about PCI DSS compliance. As shown in Bar Chart 11, all results are at or below 50 percent suggesting a net negative or unfavorable response.

Bar Chart 11: Respondents' perceptions about compliance with PCI DSS.

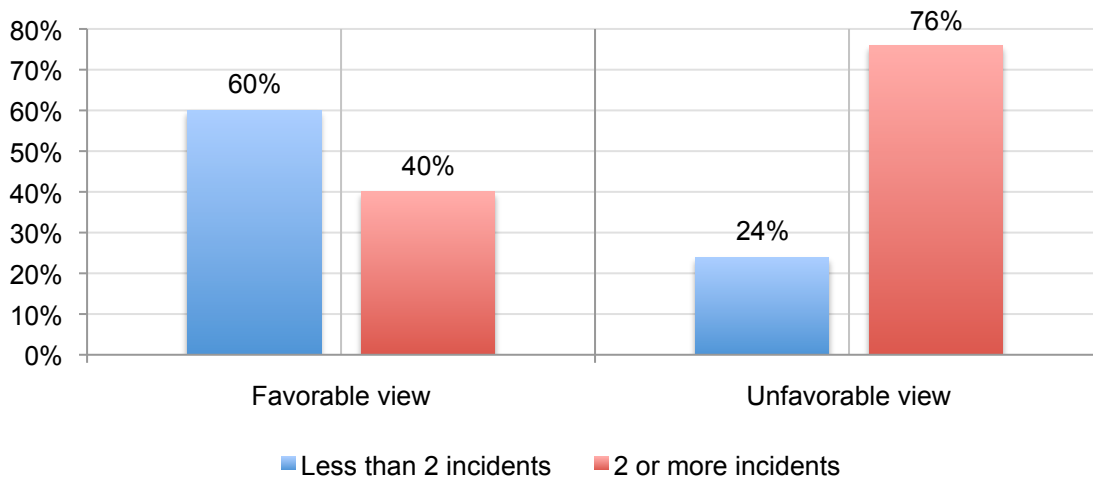
Attributions measured on a five-point scale from strongly agree to strongly disagree.



Albeit only small changes between the 2011 and 2009 results, respondents' positive perceptions about PCI DSS have declined. Most notably, in 2009 40 percent of respondents agreed that their organization had sufficient resources to achieve compliance with PCI DSS. In this year's study, the percentage of respondents has dropped to 38 percent. In 2009, 44 percent of respondents agreed that PCI DSS improved their organization's data security. This percentage also has dropped and is now at 41 percent of respondents.

In the following analysis, we looked at data breach experience between respondents who hold a favorable view about PCI DSS compliance versus those that do not hold a favorable view.³ What we learned from this cross-tabulation analysis is that respondents who hold positive perceptions about PCI compliance and its ability to improve their security posture generally have no or fewer data breaches than those who have an unfavorable view. Specifically, 40 percent of respondents from the favorable group say they had more than two incidents while 76 percent of the unfavorable group had more than two incidents.

Bar Chart 12: Data breach experience for respondents in the favorable and unfavorable groups.



Favorable perceptions also influence the level of compliance achieved in the organization. Fifty percent of the favorable respondents say that they are compliant with PCI DSS requirements across the enterprise. Among the unfavorable group, only 22 percent have achieved this level of compliance.

Organizations are moving toward endpoint encryption solutions and away from code review or debugging systems as technologies that enable compliance with PCI DSS.

Table 2 provides a list of technologies used by respondents' companies to achieve compliance with PCI DSS. This list is reported in descending order of differences between the 2011 and 2009 studies. As can be seen, the use of endpoint encryption solutions has sharply increased by 14 percent between 2009 and 2011 and anti-virus & anti-malware increased 9 percent during this period followed by firewalls and Web application firewalls (WAF) that increased 6 percent in use. Technologies that showed the greatest decline in use include an 8 percent drop in code review or debugging systems, a five percent drop in intrusion detection or prevention systems and virtual privacy networks (VPN).

³For cross-tabulation purposes, we bifurcated our sample based on all responses to Q1 in the survey instrument. In total, 168 respondents answered all six attributions as favorable (strongly agree or agree) and 184 respondents answered all attributions with strongly disagree, disagree or unsure). Those providing mixed responses were removed from this analysis.

In general, the most widely used enabling technologies have stayed consistent in the past two years. These are firewalls, anti-virus & anti-malware solutions, encryption for data-at-rest and encryption for data-in-motion.

Table 2 Technologies used by respondents' companies to achieve compliance with PCI DSS requirements.	FY 2011	FY 2009	Net change
Endpoint encryption solution	54%	40%	14%
Anti-virus & anti-malware solution	82%	73%	9%
Web application firewalls (WAF)	50%	44%	6%
Firewalls	99%	93%	6%
Identity & access management systems	55%	50%	5%
Correlation or event management systems (SIEM)	36%	31%	5%
Data loss prevention systems	30%	28%	2%
Database scanning and monitoring	43%	42%	1%
Website sniffer or crawlers	8%	9%	-1%
Encryption for data at rest	64%	65%	-1%
Encryption for data in motion	63%	64%	-1%
ID & credentialing system	26%	27%	-1%
Traffic intelligence systems	11%	13%	-2%
Access governance systems	51%	55%	-4%
Perimeter or location surveillance systems	29%	33%	-4%
Intrusion detection or prevention systems	32%	37%	-5%
Virtual privacy network (VPN)	35%	40%	-5%
Code review or debugging systems	50%	58%	-8%

Table 3 provides cross-tab results among a subset of the security enabling technologies listed above for the compliant and non-compliant group (2011 data only). There are marked differences in the enabling technologies used by these two groups. Specifically, compliant companies are more likely than non-compliant companies to use access governance systems (Diff=26 percent), anti-virus/anti-malware solutions (Diff=25 percent), Web application firewalls (Diff=16 percent), and traffic or network intelligence systems (Diff=13 percent).

Table 3 Technologies used by respondents' companies to achieve compliance with PCI DSS requirements (FY 2011 data).	Compliant	Non-compliant	Difference
Access governance systems	60%	34%	26%
Anti-virus & anti-malware solution	90%	65%	25%
Web application firewalls (WAF)	55%	39%	16%
Traffic intelligence systems	16%	2%	13%
Identity & access management systems	58%	50%	8%
Endpoint encryption solution	57%	49%	8%
Encryption for data in motion	66%	58%	8%
Correlation & event management systems (SIEM)	38%	32%	7%
Intrusion detection or prevention systems	34%	28%	7%
ID & credentialing system	28%	22%	5%
Encryption for data at rest	66%	61%	5%

PCI DSS requirements for cardholder data security differ in their level of compliance difficulty.

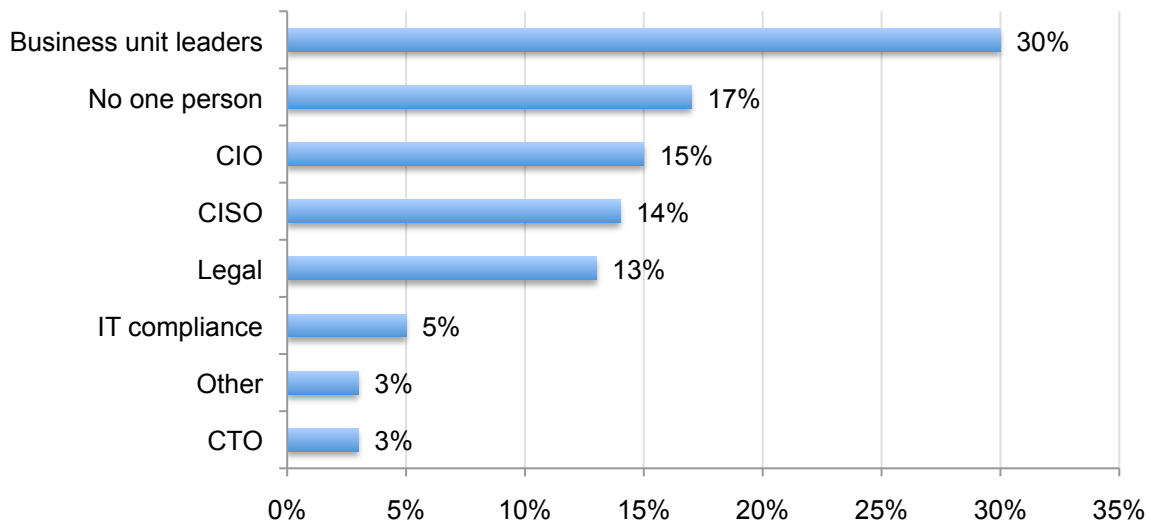
Table 4 lists 12 PCI DSS high-level compliance requirements in ascending order based on perceived difficulty according to respondents. As reported, the most difficult requirement is restricting access to confidential data by need-to-know only followed by developing and maintaining secure systems and applications and protecting stored confidential data. Least difficult are not using vendor-supplied defaults for system passwords and other security parameters, maintaining a policy that addresses data security and assigning a unique ID to each person with computer access.

Table 4 PCI DSS high-level compliance requirements for cardholder data security.	Most difficult	Least difficult
Restrict access to confidential data by need-to-know only	49%	7%
Develop and maintain secure systems and applications	45%	4%
Protect stored confidential data	41%	11%
Restrict physical access to confidential data	32%	14%
Track and monitor all access to network resources and confidential data	32%	17%
Encrypt transmission of confidential data across open, public networks	28%	20%
Regularly test security systems and processes	23%	12%
Use and regularly update anti-virus software	21%	23%
Install and maintain a firewall configuration to protect confidential data	13%	43%
Maintain a policy that addresses data security	7%	50%
Assign a unique ID to each person with computer access	4%	46%
Do not use vendor-supplied defaults for passwords and other parameters	4%	54%

Business units drive organizations' efforts to comply with PCI DSS.

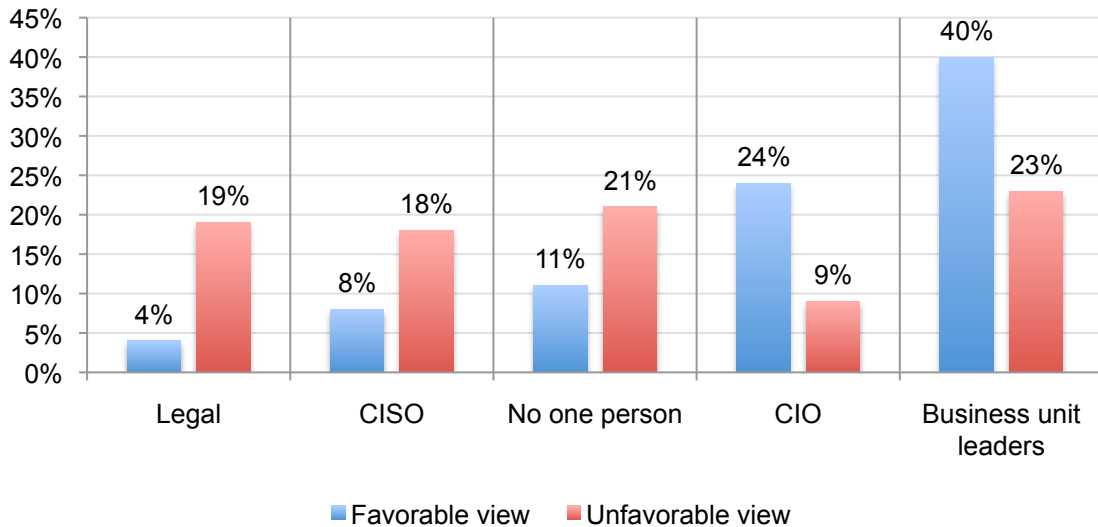
Who is most responsible for ensuring compliance with PCI DSS requirements? Thirty percent of respondents say business unit leaders are most responsible for ensuring compliance with PCI DSS requirements, followed by no one person at 17 percent. Fifteen percent say it is the CIO and 14 percent say it is the IT security leader.

Bar Chart 13: The most responsible parties for ensuring PCI DSS compliance



As noted in Bar Chart 14, respondents who hold favorable impressions about PCI DSS are more likely to have the business unit leader responsible for ensuring compliance. Forty percent of the favorable group report the business unit leader is in charge followed by 24 percent who say the CIO is in charge. In contrast, 23 percent of the unfavorable group reports that the business unit leader is in charge and 21 percent say “no one person in charge.”

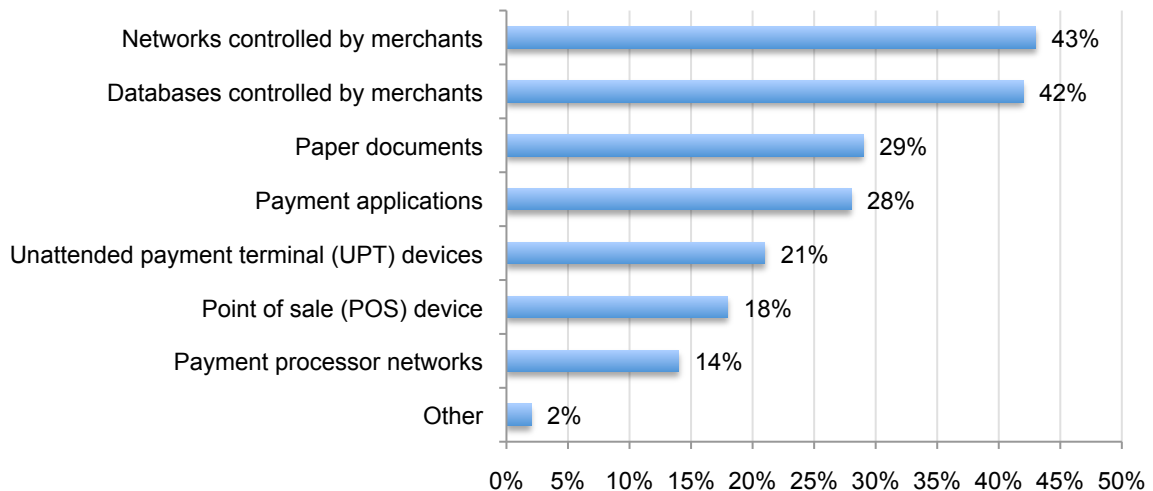
Bar Chart 14: The most responsible parties for respondents in the favorable and unfavorable groups



The most serious threats to cardholder data are located in networks and databases controlled by merchants.

Bar Chart 15 shows that 43 percent of respondents say networks controlled by merchants and 42 percent say databases controlled by merchants are where the most serious threats are located. Other areas of vulnerability include paper documents and payment applications.

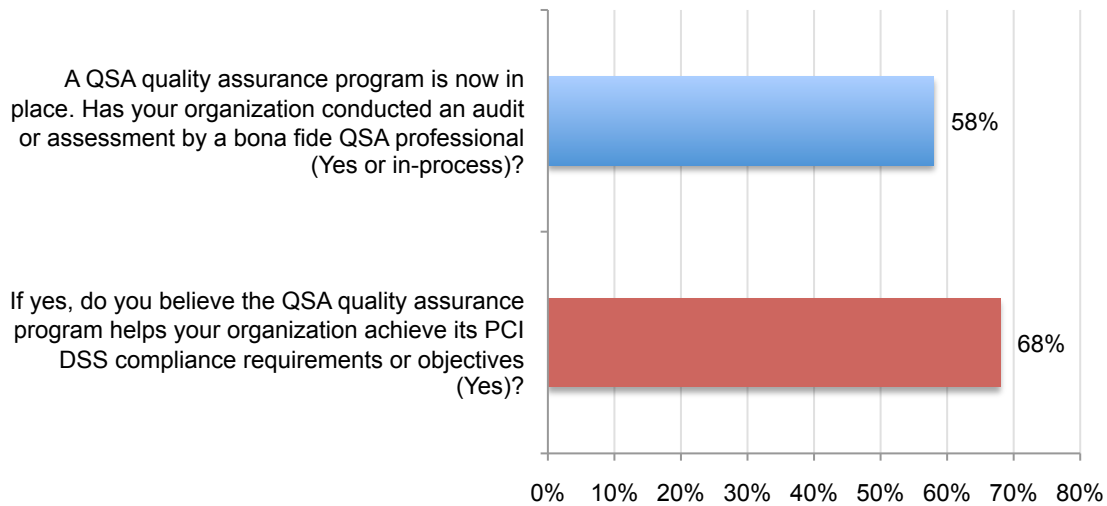
Bar Chart 15: With respect to the security of cardholder data, where are the most serious threats located?



IT and IT security practitioners view the PCI quality assurance program positively.

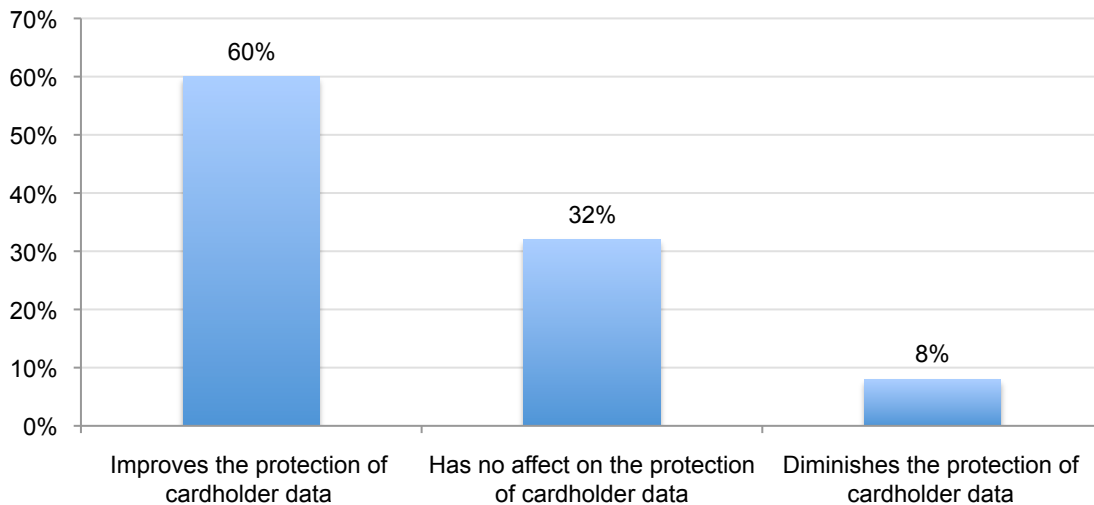
Bar Chart 16 shows 58 percent of respondents say that their organization has conducted or is in the process of conducting an audit or assessment by a bona fide QSA professional. Of those who have completed such an audit or assessment, 68 percent say that it helped the organization achieve its PCI DSS compliance requirements. While not shown in this chart, only 12 percent say it was not helpful and 20 percent are unsure.

Bar Chart 16: Experience and perceptions about the QSA program



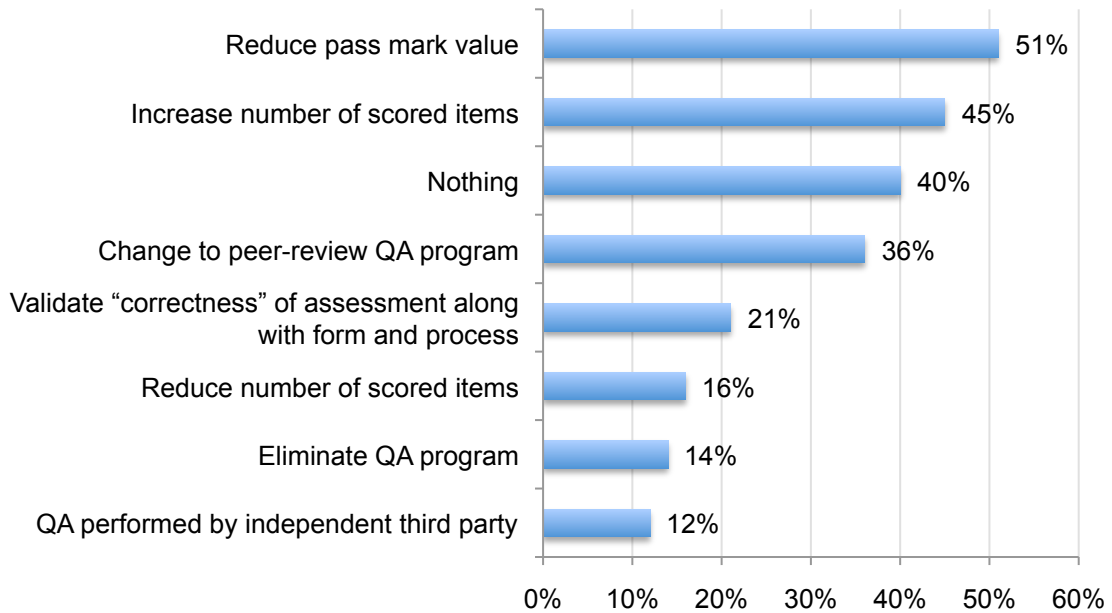
As noted in Bar Chart 17, 60 percent of respondents say that the QSA quality assurance program improves the protection of cardholder data. Another 32 percent say it has no affect on the protection of cardholder data. Only 8 percent believe the QSA program diminishes the protection of cardholder data.

Bar Chart 17: Respondents' view on how the QSA quality assurance program affects the security of cardholder data in their organization



Bar Chart 18 provides a list of changes that respondents see as important for improving the QSA program. As shown, 40 percent say nothing should be done to improve the program. However, more than half (51 percent) say that the “pass” mark value should be reduced and 45 percent say the number of scored items should be increased.

Bar Chart 18: Respondents’ views on what can be done to improve the QSA program?



Part 3. Methods

Table 5 summarizes the sample response for this study. Our sampling frame of practitioners consisted of nearly 16,000 individuals located in the United States who have bona fide credentials in the IT or IT security fields. From this sampling frame, we invited 15,699 individuals. This resulted in 803 individuals completing the survey of which 69 were rejected for reliability issues. Our final sample before screening was 734. Another 64 individuals were removed because of sample screening procedures, thus resulting in a final sample of 670 respondents (4.2 percent response rate).

Table 5 Sample response	Freq.	Pct%
Sampling frame	15996	100.0%
Returned surveys	803	5.0%
Rejected surveys	69	0.4%
Sample before screening	734	4.6%
Final sample	670	4.2%

On average, respondents held 9.56 years of experience in either the IT or IT security fields. Thirty-two percent of respondents are female and 68 percent male. Table 6 shows the position levels of respondents. As shown, 67 percent of respondents are at or above the supervisory level.

Table 6 Respondents' organizational level	Pct%
Senior Executive	1%
Vice President	0%
Director	15%
Manager	30%
Supervisor	18%
Technician	28%
Associate/Staff	5%
Other	3%
Total	100%

Table 7 shows the headcount (size) of respondents' business companies or government entities. As can be seen, 47 percent of respondents are employed by larger-sized organizations with more than 5,000 individuals.

Table 7 Global headcount of respondents' organizations	Pct%
Less than 500 people	14%
500 to 1,000 people	17%
1,001 to 5,000 people	23%
5,001 to 25,000 people	21%
25,001 to 75,000 people	15%
More than 75,000 people	10%
Total	100%

Pie Chart 2 shows the industry distribution for respondents who are employed by private and public sector organizations. As can be seen, the largest sectors include financial services (including banking, insurance, credit cards, investment management), public sector (including federal, state and local government organizations), and healthcare.

Pie Chart 2: Industry segments of respondents' organizations

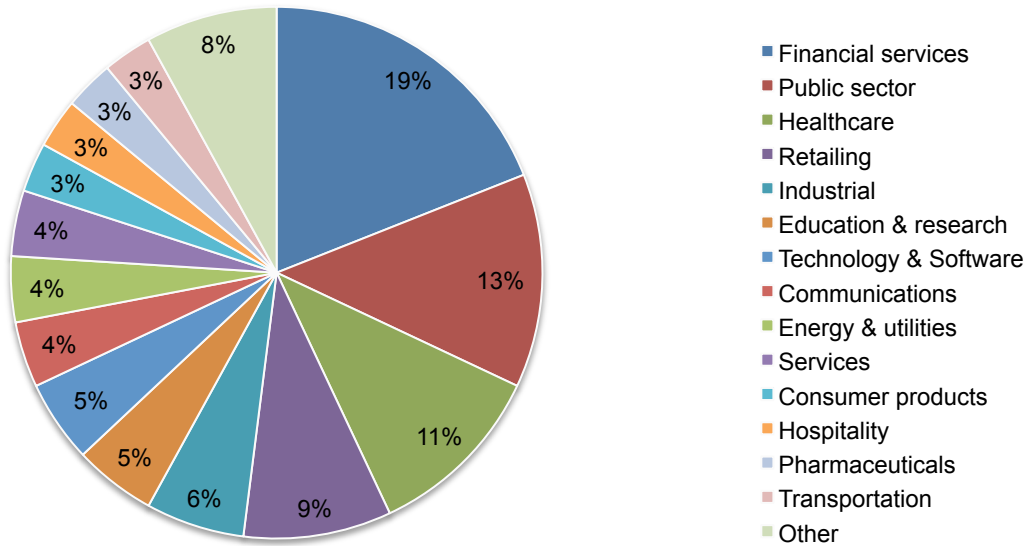


Table 8 reports the geographic footprint of respondents' organizations. In total, 76 percent of organizations have operations (headcount) in two or more countries. In addition, 65 percent have operations in one or more European nations. Finally, a total of 43 percent have operations in all major regions of the world.

Table 8 Geographic footprint of respondents' organizations	
	Pct%
United States	100%
Canada	64%
EMEA	65%
Asia-Pacific	51%
Latin America (including Mexico)	53%

Table 9 reports the PCI tier or level of validation for participating companies. As can be seen, 51 percent of organizations are classified as Tier 1 or 2 merchants. Only 9 percent are service providers.

Table 9 PCI tiers or levels of validation of respondents' organizations	
	Pct%
Tier 1 Merchant	25%
Tier 2 Merchant	26%
Tier 3 Merchant	20%
Tier 4 Merchant	20%
Tier 1 Service Provider	6%
Tier 2 Service Provider	3%
Total	100%

Part 4. Conclusion

We believe organizations have a real incentive to become PCI DSS compliant. As shown in this research, compliant organizations are more successful in reducing data breaches, especially those breaches that involve cardholder data. However, the findings also reveal that IT and IT security practitioners may not be aware of the positive impact compliance could have. Overall, respondents are not as positive in this year's study about how PCI compliance can help strengthen their organization's security posture.

As in the 2009 study, our research shows that there is very little buy-in and support from management despite the regulatory requirement. The challenge facing IT professionals is the need to make the business case for PCI-DSS so that it becomes part of the company's overall strategic initiative.

Management may become more supportive of PCI as part of an enterprise-wide security initiative if its importance to the brand and reputation of the company could be demonstrated. However, IT and IT security practitioners do not believe the connection between compliance and brand. Only 19 percent of respondents believe PCI compliance is valuable to improving brand and market place reputation. In the 2009 study we recommended that organizations display a logo that shows they are PCI compliant to create awareness among customers about what the company is doing to prevent credit card fraud. Such a strategy may prove how PCI can increase customer loyalty and reduce turnover.

Finally, we believe it is important to assign a clear champion who is accountable and responsible for both PCI and the enterprise-wide security program. This champion, by virtue of his or her position, should be empowered to direct numerous cross-functional teams to ensure broad support for PCI. An important goal of these teams will be to build a business case that results in the resources needed to ensure that it is an integral part of the company's overall security initiative.

Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- **Non-response bias**: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that auditors who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.
- **Sampling-frame bias**: The accuracy is based on contact information and the degree to which the list is representative of individuals who are information system auditors. We also acknowledge that responses from paper, interviews or telephone might result in a different pattern of findings.
- **Self-reported results**: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process, there is always the possibility that certain respondents did not provide responses that reflect their true opinions.

Appendix: Detailed Survey Findings

The following tables provide the percentage frequencies of responses to our survey instrument completed in April 2011. Several of the items are compared to items from an earlier study completed in September 2009.

Total response	Freq.	Pct%
Sampling frame	15,996	100.0%
Returned surveys	803	5.0%
Rejected surveys	69	0.4%
Sample before screening	734	4.6%
Final sample	670	4.2%

Part 1. Screening

S1. Are you responsible for managing all or part of your organization's PCI DSS compliance efforts?	Freq.	Pct%
Yes	670	91%
No (STOP)	64	9%
Total	734	100%

Part 1. Attributions. Please rate each one of the following five statements using the scale provided below each item.	Strongly agree & agree	
	FY 2011	FY 2009
Q1a. My organization has sufficient resources to achieve compliance with PCI DSS.	38%	40%
Q1b. My organization's CEO is a strong supporter of PCI DSS compliance efforts.	45%	45%
Q1c. My organization views data security as a strategic initiative across the enterprise.	25%	29%
Q1d. My organization is proactive in managing privacy and data protection risks.	44%	48%
Q1e. Compliance with PCI DSS improves our organization's data security.	41%	44%
Q1e. My organization views PCI DSS as a burden.	50%	NA

Part 2. Experience

Q2. PCI has different tiers or levels of validation. Which validation tier is required for your organization?	FY 2011	FY 2009
Tier 1 Merchant	25%	22%
Tier 2 Merchant	26%	24%
Tier 3 Merchant	20%	24%
Tier 4 Merchant	20%	23%
Tier 1 Service Provider	6%	4%
Tier 2 Service Provider	3%	3%
Total	100%	100%

Q3. Who in your organization is most responsible for ensuring compliance with PCI DSS requirements? Please select one response.	FY 2011	FY 2009
No one person	17%	21%
CIO	15%	19%
CTO	3%	8%
Business unit leaders	30%	NA
IT security leader (CISO)	14%	23%
Privacy officer or leader (CPO)	1%	2%
IT compliance	5%	9%
Internal audit	1%	2%
Legal	13%	15%
Other (please specify)	1%	2%
Total	100%	100%

Q4. Who in your organization is involved in ensuring compliance with PCI DSS requirements? Please select all that apply.	FY 2011	FY 2009
No one person	18%	21%
CIO	50%	59%
CTO	10%	14%
Business unit leaders	67%	NA
IT security leader (CISO)	36%	34%
Privacy officer or leader (CPO)	11%	16%
IT compliance	20%	19%
Internal audit	22%	23%
Legal	35%	37%
Other (please specify)	1%	2%
Total	273%	225%

Q5. Is your organization compliant with PCI DSS requirements today?	FY 2011	FY 2009
Yes, for all applications and databases across the enterprise	33%	22%
Yes, for most applications and databases across the enterprise	33%	28%
Yes, but only for some applications and databases across the enterprise	18%	25%
No	16%	25%
Total	100%	100%

Q6. Did your organization ever fail a PCI DSS audit or assessment?	FY 2011
Yes	4%
No	96%
Total	100%

Q7. How important are compensating controls to the fulfillment of the following 12 PCI DSS requirements in your organization? Please rate each requirement using the adjacent scale.	FY 2011 Data		
	Critical	Convenient	Irrelevant
Install and maintain a firewall configuration to protect confidential data	66%	32%	2%
Do not use vendor-supplied defaults for system passwords and other security parameters	58%	28%	14%
Protect stored confidential data	59%	35%	6%
Encrypt transmission of confidential data across open, public networks	33%	49%	18%
Use and regularly update anti-virus software	60%	29%	11%
Develop and maintain secure systems and applications	35%	52%	13%
Restrict access to confidential data by need-to-know only	32%	51%	17%
Assign a unique ID to each person with computer access	28%	27%	45%
Restrict physical access to confidential data	25%	56%	19%
Track and monitor all access to network resources and confidential data	30%	48%	22%
Regularly test security systems and processes	33%	52%	15%
Maintain a policy that addresses data security	29%	63%	8%
Average	41%	44%	16%

Q8a. How many data breaches has your organization experienced in the past 24 months?	FY 2011	FY 2009
None	15%	21%
1 incident	33%	38%
2 to 5 incidents	41%	30%
More than 5 incidents	11%	11%
Total	100%	100%

Q8b. How many data breaches has your organization experienced involving the loss or theft of cardholder data in the past 24 months?	FY 2011
None	55%
1 incident	39%
2 to 5 incidents	6%
More than 5 incidents	0%
Total	100%

Q9. In your opinion, did your organization's data breach experience decline as a result of its compliance with PCI DSS?	FY 2011
Yes	12%
No	38%
Unsure	50%
Total	100%

Part 3. Cardholder data protection

Q10. With respect to the security of cardholder data, where are the most serious threats located? Please select only two top choices.	FY 2011
Point of sale (POS) device	18%
Unattended payment terminal (UPT) devices	21%
Payment processor networks	14%
Networks controlled by merchants	43%
Databases controlled by merchants	42%
Payment applications	28%
Paper documents	29%
Other (please specify)	2%
Total	197%

Following are 12 PCI DSS high-level compliance requirements for cardholder data security. From the list below, please select the three most and least difficult requirements to comply with.	FY 2011 Data	
	Q11a Most difficult	Q11b. Least difficult
Restrict access to confidential data by need-to-know only	49%	7%
Develop and maintain secure systems and applications	45%	4%
Protect stored confidential data	41%	11%
Restrict physical access to confidential data	32%	14%
Track and monitor all access to network resources and confidential data	32%	17%
Encrypt transmission of confidential data across open, public networks	28%	20%
Regularly test security systems and processes	23%	12%
Use and regularly update anti-virus software	21%	23%
Install and maintain a firewall configuration to protect confidential data	13%	43%
Maintain a policy that addresses data security	7%	50%
Assign a unique ID to each person with computer access	4%	46%
Do not use vendor-supplied defaults for system passwords and other security parameters	4%	54%
Total	300%	300%

Q12a. Does your organization retain and store PAN (primary account numbers)?	FY 2011
Yes	66%
No	34%
Total	100%

Q12b. If yes, why does your organization retain and store PAN (primary account number)? Please select the top two business reasons.	FY 2011
Recurring subscriptions	31%
Charge backs	45%
Card reuse	49%
Customer service	52%
Marketing analytics	19%
Other	3%
Total	199%

Q13. Please select all the technologies in your organization that enable compliance with PCI DSS requirements.	Yes % FY 2011	Yes % FY 2009	Net change
Endpoint encryption solution	54%	40%	14%
Anti-virus & anti-malware solution	82%	73%	9%
Web application firewalls (WAF)	50%	44%	6%
Firewalls	99%	93%	6%
Identity & access management systems	55%	50%	5%
Correlation or event management systems (SIEM)	36%	31%	5%
Data loss prevention systems	30%	28%	2%
Database scanning and monitoring	43%	42%	1%
Website sniffer or crawlers	8%	9%	-1%
Encryption for data at rest	64%	65%	-1%
Encryption for data in motion	63%	64%	-1%
ID & credentialing system	26%	27%	-1%
Traffic intelligence systems	11%	13%	-2%
Access governance systems	51%	55%	-4%
Perimeter or location surveillance systems	29%	33%	-4%
Intrusion detection or prevention systems	32%	37%	-5%
Virtual privacy network (VPN)	35%	40%	-5%
Code review or debugging systems	50%	58%	-8%

Q13. For all the technologies used in your organization that enable compliance, indicate the relative cost effectiveness of each technology with respect to achieving PCI DSS compliance goals by using one of three choices: high, moderate or low.	Hi% FY 2011	Hi% FY 2009	Net Change
Access governance systems	65%	62%	3%
Anti-virus & anti-malware solution	69%	74%	-5%
Code review or debugging systems	45%	59%	-14%
Correlation or event management systems (SIEM)	41%	30%	11%
Data loss prevention systems	43%	45%	-2%
Database scanning and monitoring	48%	51%	-3%
Encryption for data at rest	69%	73%	-4%
Encryption for data in motion	80%	78%	2%
Endpoint encryption solution	51%	45%	6%
Firewalls	95%	98%	-3%
ID & credentialing system	42%	37%	5%
Identity & access management systems	64%	56%	8%
Intrusion detection or prevention systems	39%	42%	-3%
Perimeter or location surveillance systems	40%	37%	3%
Traffic intelligence systems	25%	12%	13%
Virtual privacy network (VPN)	52%	48%	4%
Web application firewalls (WAF)	67%	62%	5%
Website sniffer or crawlers	6%	5%	1%

Part 4. PCI Quality Assurance Program

Q14a. A QSA quality assurance program is now in place. Has your organization conducted an audit or assessment by a bona fide QSA professional?	FY 2011
Yes	46%
In-process	12%
No (go to Part 5)	42%
Total	100%

Q14b. If yes, do you believe the QSA quality assurance program helps your organization achieve its PCI DSS compliance requirements or objectives?	FY 2011
Yes	68%
No	12%
Unsure	20%
Total	100%

Q14c. If no or unsure, please explain why?	FY 2011
QSAs do not possess the qualifications to assess compliance	54%
The scope of the audit or assessment is inadequate	23%
The audit or assessment standards are inadequate	18%
Lack of enforcement	36%
Other (please specify)	5%
Total	136%

Q14d. In your opinion, how does PCI's QSA quality assurance program affect the security of cardholder data in your organization?	FY 2011
Improves the protection of cardholder data	60%
Has no affect on protection of cardholder data	32%
Diminishes the protection of cardholder data	8%
Total	100%

Q14e. What do you believe should be done to improve the QSA quality assurance program? Please select all that apply.	FY 2011
Change to peer-review QA program	36%
QA performed by independent third party (separate from PCI DSS)	12%
Eliminate QA program	14%
Validating "correctness" of assessment along with form and process	21%
Reducing number of scored items	16%
Increasing number of scored items	45%
Reducing "pass" mark value	51%
Other	5%
Nothing	40%
Total	240%

Part 5. Budget

Q15. What dollar range best describes your organization's IT security budget in the present fiscal year?	FY 2011	FY 2009
Less than \$1 million	2%	5%
Between \$1 to 2 million	3%	4%
Between \$3 to \$4 million	5%	3%
Between \$5 to \$6 million	6%	7%
Between \$7 to \$8 million	7%	7%
Between \$9 to \$10 million	4%	3%
Between \$11 to \$12 million	11%	10%
Between \$13 to \$14 million	12%	10%
Between \$15 to \$16 million	11%	13%
Between \$17 to \$18 million	0%	0%
Between \$19 to \$20 million	0%	1%
Over \$20 million	39%	38%
Total	100%	100%
Extrapolated value in \$millions	14.64	14.27

Q16. What percentage of the current IT security budget will go to achieving PCI DSS compliance?	FY 2011	FY 2009
Less than 5%	4%	4%
Between 5% to 10%	3%	5%
Between 10% to 20%	5%	8%
Between 20% to 30%	15%	15%
Between 30% to 40%	32%	32%
Between 40% to 50%	21%	20%
Between 50% to 60%	10%	7%
Between 60% to 70%	8%	4%
Between 70% to 80%	0%	0%
Between 80% to 90%	2%	3%
Between 90% to 100%	0%	0%
Total	100%	100%
Extrapolated average percentage	38%	35%

Q17. What percentage of the traditional IT security budget has shifted or been moved to PCI DSS compliance goals?	FY 2011	FY 2009
Less than 5%	15%	16%
Between 5% to 10%	9%	8%
Between 10% to 20%	20%	16%
Between 20% to 30%	15%	17%
Between 30% to 40%	12%	13%
Between 40% to 50%	7%	5%
Between 50% to 60%	6%	3%
Between 60% to 70%	0%	2%
Between 70% to 80%	0%	0%
Between 80% to 90%	2%	3%
Between 90% to 100%	14%	17%
Total	100%	100%
Extrapolated average percentage	34%	36%

Q18. Please choose one statement that best describes the value of PSI DSS expenditures to your organization.	FY 2011
PCI DSS compliance contributes more value than expenditures made.	33%
PCI DSS compliance contributes about the same value as expenditures made.	35%
PCI DSS compliance contributes less value than expenditures made.	32%
Total	100%

Q19. Please select the value PCI DSS compliance provides your organization. Check all that applies.	FY 2011	FY 2009
Improves our organization's data security posture.	39%	45%
Improves our organization's marketplace brand and reputation.	19%	21%
Improves our organization's relationship with key business partners.	66%	64%
Heightens awareness among C-levels within our organization.	35%	33%
Helps secure more funding for IT security.	59%	63%
Other (please specify)	0%	0%
Total	218%	226%

Q20. What is the purpose of security compliance programs such as PCI DSS, ISO, NIST and other related initiatives. Please choose the statements you believe to be true about compliance.	FY 2011	FY 2009
Not necessary.	33%	36%
Only "CYA."	28%	33%
Necessary to achieve consistent security practices across the enterprise.	35%	30%
Necessary to obtain buy-in from management.	48%	47%
Necessary to secure security budget and funding.	56%	52%
Necessary to prioritize security requirements.	49%	46%
Essential to achieving an effective security posture.	44%	48%
Total	293%	292%

Following is a list of compliance requirements for many organizations in the United States. Please select the three compliance requirements that are most/least difficult to achieve within your organization.	FY 2011 Data	
	Q21a. Most difficult	Q21b. Least difficult
PCI DSS	53%	21%
HIPAA (including HITECH)	32%	15%
Sarbanes-Oxley	48%	14%
Gramm-Leach-Bliley (GLBA)	7%	60%
ISO standards	25%	15%
NIST standards	26%	5%
Fair Information Practices (FTC)	2%	55%
Fair Credit Reporting Act (FCRA)	5%	25%
FISMA	9%	4%
EU Data Protection Directive (including Safe Harbor)	12%	57%
Various US state privacy and data protection laws	39%	13%
Various national privacy and data protection laws	40%	17%
Total	300%	300%

Part 6. Your role

D1. What organizational level best describes your current position?	FY 2011
Senior Executive	1%
Vice President	0%
Director	15%
Manager	30%
Supervisor	18%
Technician	28%
Associate/Staff	5%
Other	3%
Total	100%

D2. Is this a full time position?	FY 2011
Yes	98%
No	2%
Total	100%

D3. Check the Primary Person you or your IT security leader reports to within the organization.	FY 2011
CEO/Executive Committee	0%
Chief Financial Officer	4%
General Counsel	2%
Chief Information Officer	56%
Chief Information Security Officer (CISO)	16%
Compliance officer	11%
Human Resources VP	0%
Chief Security Officer (CSO)	5%
Chief Risk Officer	6%
Other	0%
Total	100%

D4. Experience	Mean	Median
Total years of IT or IT security experience	9.56	10.00
Total years in current position	3.93	4.50

D5. Gender	FY 2011
Female	32%
Male	68%
Total	100%

D6. What industry best describes your organization's industry focus?	FY 2011
Financial services	19%
Public sector	13%
Healthcare	11%
Retailing	9%
Industrial	6%
Education & research	5%
Technology & Software	5%
Communications	4%
Energy & utilities	4%
Services	4%
Consumer products	3%
Hospitality	3%
Pharmaceuticals	3%
Transportation	3%
Chemicals	2%
Defense	2%
Media	2%
Agriculture	1%
Other	1%
Total	100%

D7. Where are your employees located? (Check all that apply):	FY 2011
United States	100%
Canada	64%
EMEA	65%
Asia-Pacific	51%
Latin America (including Mexico)	53%

D8. The scope of PCI DSS efforts (check all that apply):	FY 2011
United States	100%
Canada	55%
EMEA	21%
Asia-Pacific	19%
Latin America (including Mexico)	15%

D9. What is the worldwide headcount of your organization?	FY 2011
Less than 500 people	14%
500 to 1,000 people	17%
1,001 to 5,000 people	23%
5,001 to 25,000 people	21%
25,001 to 75,000 people	15%
More than 75,000 people	10%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.