



2009 PCI DSS Compliance Survey

Sponsored by Imperva

Independently conducted by Ponemon Institute LLC

Publication Date: September 24, 2009

2009 PCI DSS Compliance Study

By Ponemon Institute, September 24, 2009

Executive Summary

PCI was devised to help improve credit card security and protect consumers and card issuers from fraud. The *2009 PCI DSS Compliance* study was conducted by Ponemon Institute and sponsored by Imperva to determine if PCI compliance improves organizational security. More specifically, the study seeks to determine how the move to comply with PCI affects an organization's strategy, tactics and approach to achieving enterprise data protection and security.

In general, the findings show that PCI-DSS compliance is perceived as contributing to an organization's security posture. However, the main obstacle for PCI-DSS compliance is cost. For that reason, compliance is stronger with larger, more budgeted organizations that adopt cost-effective solutions to achieve compliance.

A total of 517 United States and multinational IT and IT security practitioners who are involved in their companies' PCI compliance efforts were surveyed on the following topics:

- Who is most responsible in an organization for ensuring compliance with PCI DSS requirements?
- What technologies enable compliance with PCI DSS requirements?
- What is the scope of compliance with PCI DSS?
- Does PCI DSS decrease, have no impact or increase security threats?
- What is the value PCI DSS compliance provides to the organization?

Following are the most salient findings of this survey research. We have organized the report into three parts: Part 1 presents the key findings of the survey and Part 2 discusses the evolutionary or maturity stages an organization adopts for its data security strategy and how these stages explain its compliance with PCI DSS. These stages were determined by how respondents in the study perceived their organization's attitudes about such issues as support from the CEO, being proactive about privacy and data protection and having sufficient resources for PCI DSS compliance. Part 3 provides recommendations.

Please note that most of the results are displayed in bar chart format. The actual data utilized in each figure and referenced in this paper can be found in the percentage frequency tables attached as the Appendix to this paper.

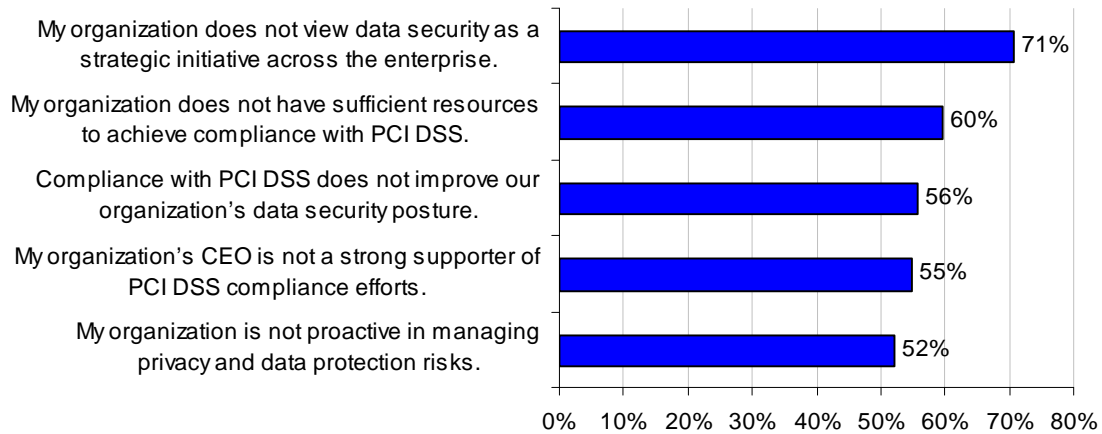
Part 1: Key Findings

The survey finds that 71 percent of companies do not treat PCI as a strategic initiative and 79 percent have experienced a data breach.

In general, respondents in this study do not have what could be considered a favorable view of their organization's security posture. For example, 71 percent do not believe their organization views data security as a strategic initiative across the enterprise, and 55 percent do not believe their CEO has strong support for PCI DSS compliance efforts. In addition, 52 percent do not believe their organization is proactive in managing privacy and data protection risks.

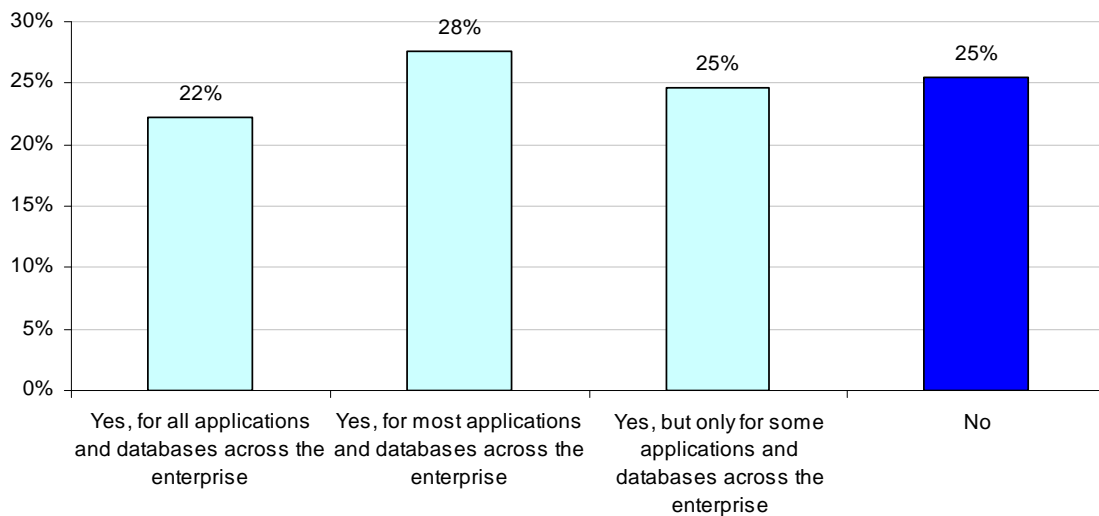
Fifty-six percent of respondents do not believe compliance with PCI DSS improves their organization's data security posture, and 60 percent say their organization does not have sufficient resources to achieve compliance with PCI DSS. See Bar Chart 1.

Bar Chart 1
Attributions about the organization's PCI data security posture



Despite this less than favorable orientation to PCI DSS, 75 percent of respondents say their organizations have achieved some level of compliance. Accordingly, 28 percent are compliant for most applications and databases across the enterprise, while 25 percent are compliant for some applications and databases. Twenty-two percent of respondents say their organizations have achieved full PCI DSS compliance for applications and databases across the enterprise.

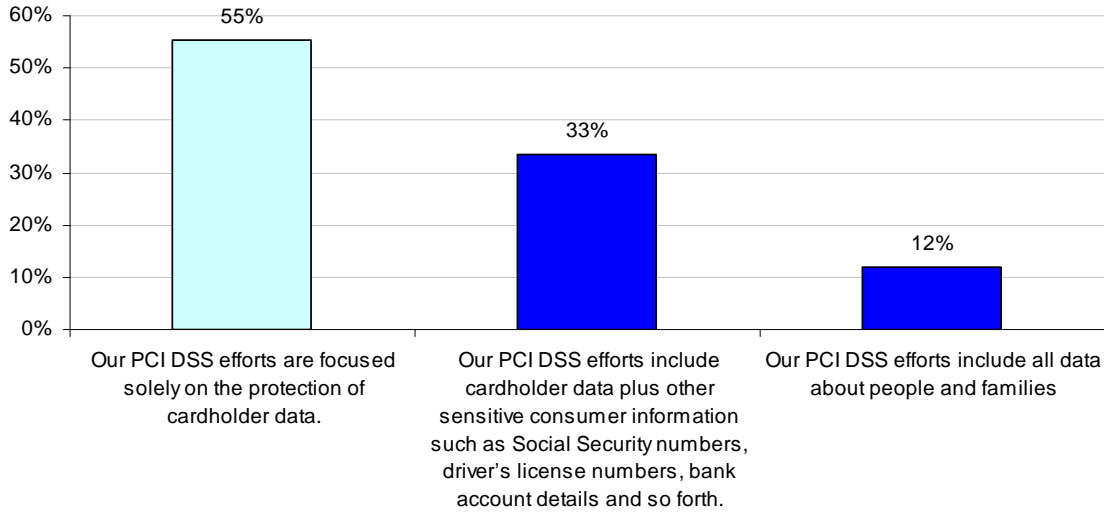
Bar Chart 2
Organizations compliant with PCI DSS requirements today



Today, 55 percent focus only on credit card data protection and do not attempt to secure sensitive information such as Social Security Numbers, driver's license numbers, bank account details and other personal data

PCI only address the protection of credit card information. More than half of respondents (55 percent) admit to not protect data outside the minimum credit card data protection PCI covers. Forty-five percent say the have an expanded program that goes beyond the baseline PCI data protection requirements. These findings are shown in Bar Chart 2.

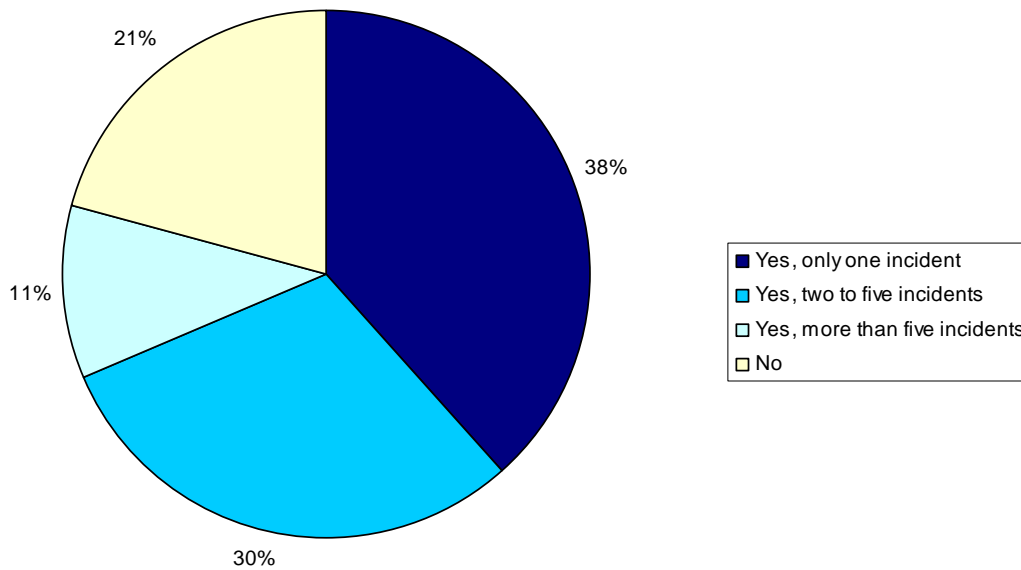
Bar Chart 2
Focus of PCI DSS compliance efforts



The majority of organizations in this study have had a data breach.

Seventy-nine percent of organizations in our study had at least one data breach. Only 21 percent reported that they had none (Pie Chart 1). Of those respondents who report their organizations experienced one or more data breaches, 64 percent had to publicly disclose the data breach (20 percent for all data breach incidents and 44 percent for some data breach incidents). Thirty-six percent say no disclosure was deemed to be necessary (not shown in pie chart).

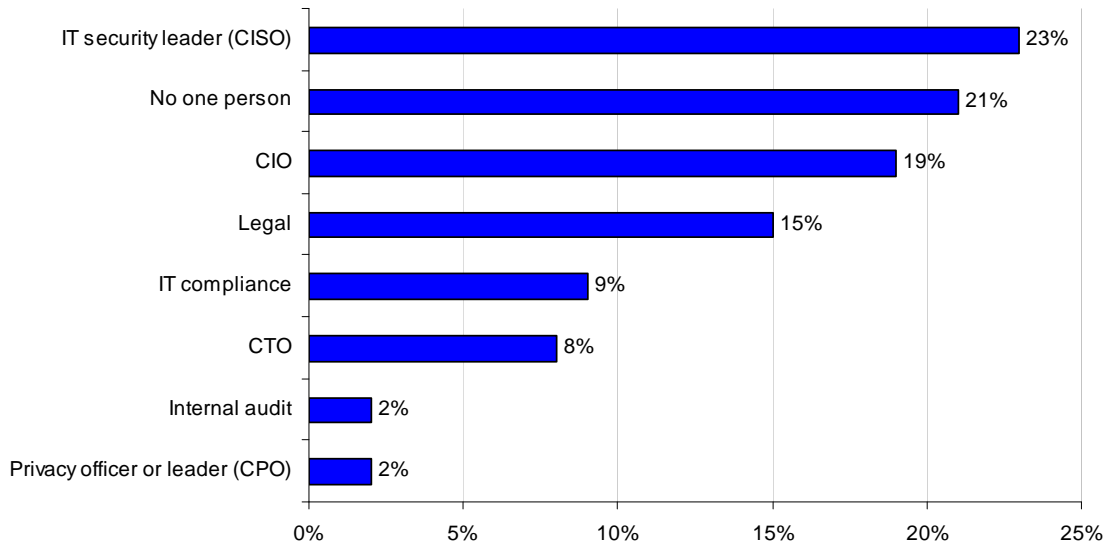
Pie Chart 1
Data breach experience



There is uncertainty as to who is most responsible for PCI DSS compliance. Twenty-three percent say it is the CISO followed by no one person (21 percent) and the CIO (19 percent).

Bar Chart 3 shows there is uncertainty as to who is most responsible for security compliance. This uncertainty suggests there is a lack of accountability and leadership for ensuring PCI compliance. Least responsible for PCI compliance is: IT compliance (9 percent), chief technology officer (8 percent), internal audit (2 percent) and the privacy leader (2 percent).

**Bar Chart 3
Data breach experience**



The following technologies enable PCI DSS compliance and are the most cost effective.

Table 1 Technologies in ascending order by average cost effectiveness rating	Pct%*
Firewalls	82%
Anti-virus & anti-malware solutions	74%
Encryption for data at rest	74%
Encryption for data in motion	71%
Access governance systems	64%
Identity & access management systems	63%
Web application firewalls (WAF)	55%
Correlation or event management systems	55%
Endpoint encryption solution	46%
Data loss prevention systems	43%
Code review	36%
Traffic intelligence systems	32%
Virtual privacy network (VPN)	26%
Intrusion detection or prevention systems	22%
Database scanning and monitoring	18%
ID & credentialing system	11%
Website sniffer or crawlers	7%
Perimeter or location surveillance systems	3%
Average	43%

*Pct% defines the average percentage of respondents rating the technology as highly cost effective.

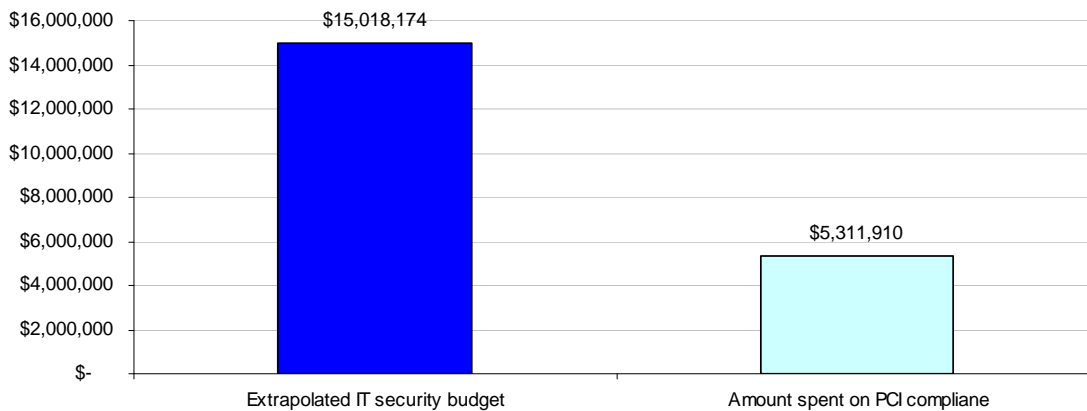
As shown in Table 1, firewalls, anti-virus and anti-malware solutions and encryption for data at rest are the top three technologies that enable compliance with PCI DSS. These are ranked highest by respondents as cost-effective technologies.

Technologies least used are traffic intelligence and website sniffers or crawlers. ID & credentialing systems and perimeter or location surveillance systems are considered least effective in achieving PCI DSS requirements.

The cost of PCI is about one-third of the overall security budget.

PCI was one way to get funding for IT security. On average, companies spent about a third of their budget on PCI. The average IT security budget was approximately \$15 million, meaning most companies spend about \$5 million, as shown in Bar Chart 4. The average company size was nearly \$5 billion in annual revenue.

Bar Chart 4
Extrapolated IT security budget and spending on PCI DSS compliance



The survey also revealed that PCI helps companies shift budget from one category to another. It turns out most companies are not incrementally spending more, but basically moving budget to something that's viewed as more critical. And, again, PCI was viewed as the critical driver that organizations were likely to shift funds to in order to achieve security program goals.

Part 2: PCI Compliance Taxonomy

As we learned in the survey, companies still struggle to ensure that sensitive consumer data is protected. However, organizations do not seem to treat PCI as a strategic initiative.

To better understand why certain organizations may be more strategic than others, we decided to look at responses to the following five attributions and group respondents into one of three evolutionary stages or orientations about data security:

1. My organization has sufficient resources to achieve compliance with PCI DSS.
2. My organization's CEO is a strong supporter of PCI DSS compliance efforts.
3. My organization views data security as a strategic initiative across the enterprise.
4. My organization is proactive in managing privacy and data protection risks.
5. Compliance with PCI DSS improves our organization's data security.

This deeper analysis of the survey findings illustrate that CEOs can impact data security by making it a strategic corporate initiative. A CEO's mandate and involvement is essential for strong data protection. For example, we found that in companies where data security was a high priority, 100 percent of CEOs were aware of and supported PCI and a broad security strategy. In

companies where PCI was viewed cynically, 100 percent of CEOs were unaware or didn't support PCI.

Each attribution is rated using a five-point adjective scale from strongly agree (most favorable) to strongly disagree (least favorable). Table 2 summarizes the reclassification of the overall sample according to three discrete subgroups.

Table 2 Orientations to security or evolutionary stages	Freq	Pct%
Cynical stage (least favorable = disagree or strongly disagree)	98	19%
Checklist stage (middle of the pack = mixed responses)	279	54%
Enlightenment stage (most favorable = agree or strongly agree)	140	27%
Final sample	517	100%

The starting orientation to data security is termed the **cynical stage**. Companies in this stage are likely to view self-regulatory security initiatives such as PCI, ISO, NIST and others in a jaundiced or negative light. It is our belief that these individuals are more likely to be in denial about the extant risks or likelihood of security threats that abound their organizations. We define individuals in the first stage as those who answer all five attributions as disagree or strongly disagree. In total, 98 respondents, or 19 percent of the final sample, are classified as cynics.

Cynics can be characterized by:

- Attitude toward PCI compliance: Not important, not necessary, costs too much and only CYA.
- Organizational structure to security compliance: No ownership and limited accountability.
- Strategy: Focus only on the minimum compliance required.

Following are key attributions about respondents in the cynical stage:

- 100 percent believe their company's CEO is not a strong supporter of PCI compliance efforts.
- 85 percent believe that PCI compliance is not essential to achieving an effective security posture.
- 77 percent believe that PCI compliance is not necessary to achieving consistent security practices across the enterprise.
- 51 percent believe that PCI compliance is merely "CYA".
- 30 percent state that no one person is responsible for ensuring compliance with PCI in their companies.

Other relevant facts about cynics:

- Approximate company budget dedicated to IS security is \$12.95 million.
- About 31 percent of the total security budget is dedicated to PCI compliance.
- 68 percent say they focus PCI efforts on cardholder data only (evidence of tactical rather than strategic view).
- Overall PCI compliance rate is 40 percent.

The second orientation to data security is termed the **checklist stage**. Companies in this middle stage are more receptive to security initiatives such as PCI, but are not completely convinced that self-regulatory requirements for compliance will lead to better security. We define IT security practitioners in the second stage as those who provided mixed responses to the five attributions (i.e., some questions answered as agree, while others are answered as disagree). A total of 279 respondents, or 54 percent of the final sample, are classified as checklist.

Checklists can be characterized by:

- Attitude toward PCI compliance: Get it done, but only to the level required by standards or law.
- Organizational structure to security compliance: mid-level management owns PCI with minimal involvement from C-level executives.
- Strategy: Secure all relevant data. Achieve security goals at all costs.

Following are key attributions about respondents in the checklist stage:

- 45 percent believe their company's CEO is a strong supporter of PCI compliance efforts.
- 72 percent believe PCI compliance is essential to achieving an effective security posture.
- 70 percent believe PCI compliance is necessary to achieving consistent security practices across the enterprise.
- 67 percent believe PCI compliance is not merely "CYA".
- 12 percent state that no one person is responsible for ensuring compliance with PCI in their companies.

Other relevant facts about checklist stage:

- Approximate company budget dedicated to IS security is \$15.02 million.
- About 35 percent of the total security budget is dedicated to PCI compliance.
- 45 percent say they only focus PCI efforts on more than cardholder data.
- Overall PCI compliance rate is 50 percent.

The final and highest orientation to data security compliance is termed the **enlightenment stage**. Enlightened companies are likely to view self-regulatory security initiatives such as PCI, ISO, NIST and others in a favorable or positive light. It is our belief that these individuals are more likely to see PCI as a means to achieving real and substantial security protections, thereby reducing extant security threats across their organizations. We define individuals in the third stage as those who answer all five attributions as agree or strongly agree. In total, 140 respondents, or 27 percent of the final sample, are classified as enlightened.

Enlightenment can be characterized by:

- Attitude toward PCI compliance: PCI improves the company's overall security posture.
- Organizational structure to security compliance: Executive level ownership and oversight.
- Strategy: Maximize security bang for the buck. Focus on the enterprise.

Following are key attributions about respondents in the enlightenment stage:

- 100 percent believe their company's CEO is a strong supporter of PCI compliance efforts.
- 48 percent believe PCI compliance is essential to achieving an effective security posture.
- 45 percent believe PCI compliance is necessary to achieving consistent security practices across the enterprise.
- 87 percent believe PCI compliance is not merely "CYA".
- 21 percent state that no one person is responsible for ensuring compliance with PCI in their companies.

Other relevant facts about the enlightenment stage:

- Approximate company budget dedicated to IS security is \$18.01 million.
- About 39 percent of the total security budget is dedicated to PCI compliance.
- 54 percent say they only focus PCI efforts on more than cardholder data.
- Overall PCI compliance rate is 72 percent.

Part 3: Method

A random sampling frame of 9,958 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our randomly selected sampling frame was built from proprietary lists of experienced IT and IT security practitioners.

Table 3 Sample response	Freq.
Sampling frame	9,958
Bounce-back	1,893
Total sample (before reliability)	619
Response rate (before reliability)	6.2%
Total sample (final)	560
Response rate (final)	5.6%

In total, 619 respondents completed the survey. Of the returned instruments, 59 surveys failed reliability checks. A total of 560 surveys were used as our final sample, which represents a 5.6 percent net response rate. One screening question was used to ensure respondents had experience with PCI DSS compliance, resulting in a reduced sample size of 517 individuals.

Ninety percent of respondents completed all survey items within 14 minutes. Table 4 reports the respondent organization's PCI tier (merchants and service providers) level. As can be seen, the present sample is evenly distributed among all four merchant tiers. Only 7 percent of respondent organizations are service providers.

Table 4 Distribution of the sample by PCI DSS Tiers	Pct%
Tier 1 Merchant	22%
Tier 2 Merchant	24%
Tier 3 Merchant	24%
Tier 4 Merchant	23%
Tier 1 Service Provider	4%
Tier 2 Service Provider	3%
Total	100%

Table 5 reports the respondent organization's global headcount. As shown, a majority of respondents work within companies with more than 1,000 employees.

Table 5 The worldwide headcount of respondent organizations	Pct%
Less than 500 people	15%
500 to 1,000 people	19%
1,001 to 5,000 people	22%
5,001 to 25,000 people	20%
25,001 to 75,000 people	14%
More than 75,000 people	10%
Total	100%

Table 6 reports the respondent's primary reporting channel. As can be seen, 55 percent of respondents are located in the organization's IT department (led by the company's CIO). Only 14 percent report to the company's security officer (or CISO).

Table 6 Respondent's primary reporting channel.	Pct%
Chief Information Officer	55%
Chief Security Officer/CISO	14%
Chief Technology Officer	11%
Chief Risk Officer	8%
Chief Financial Officer	4%
Compliance Officer	3%
Human Resources VP	3%
Other	2%
Total	100%

Table 7 reports the respondent organization's global footprint. As can be seen, a large number of participating organizations are multinational companies that operate outside the United States.

Table 7 Global footprint of the respondent's organization	Pct%
United States	100%
Canada	56%
Europe	45%
Asia-Pacific	34%
Latin America (including Mexico)	26%

The average overall experience level of respondents is 10.07 years, and the years of experience in their present job is 3.16 years.

Caveats to this study

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 individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would 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 subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Part 4: Recommendations

Based on the findings of this study, we have the following recommendations:

The PCI-DSS Council should consider creating a compliance logo that companies can display. This would inform consumers that companies may be more security conscious because of their use of PCI-DSS. As a result, consumers may have more confidence in these organizations. In turn, creating consumer awareness about the importance of PCI could help companies investing in security gain a competitive advantage. This is especially important given that our research suggests that PCI compliant companies are less likely to suffer a data breach than non-PCI companies.

We also suggest that compliance requirements be tailored to the size of the organization. For example, smaller companies operate in a different environment with different security needs.

Our research also shows 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.

Senior 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. For example, displaying the logo suggested above and creating awareness among customers about what the company is doing to prevent credit card fraud can be a competitive advantage. Such a strategy may prove how PCI can increase customers and reduce turnover.

Finally, assign a clear champion who is accountable and responsible not just for PCI but for 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 it is an integral part of the company's overall security initiative.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, phone call or e-mail:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

About Ponemon Institute

The Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries. Visit the Ponemon Institute at www.ponemon.org.

About Imperva

Imperva, the Data Security leader, enables a complete security lifecycle for business databases and the applications that use them. More than 4,500 of the world's leading enterprises, government organizations, and managed service providers rely on Imperva to prevent sensitive data theft, protect against data breaches, secure applications, and ensure data confidentiality. The award-winning Imperva SecureSphere is the only solution that delivers full activity monitoring from the database to the accountable application user and is recognized for its overall ease of management and deployment. For more information, visit www.imperva.com.

2009 PCI DSS Compliance Survey

Audited results presented by Dr. Larry Ponemon, revised on September 7, 2009

The following tables provide the frequency and percentage frequency of responses to all survey questions. This web-based survey was conducted by Ponemon Institute with subject debriefing completed on September 2, 2009. The final sample size involves 560 respondents (517 after screening).

Sampling frame (U.S. IT & IT security)	9,958
Bounce-back	1,893
Total sample (before reliability)	619
Response rate (before reliability)	6.2%
Total sample (final)	560
Response rate (final)	5.6%

S1. Are you responsible for managing all or part of your organization's PCI DSS compliance efforts?	Freq
Yes	517
No (Stop)	43
Total	560

Attributions about your company where 1 = strongly agree, 2 = agree, 3 = unsure, 4 = disagree and 5 = strongly disagree.	Strongly agree & agree combined
Q1a. My organization has sufficient resources to achieve compliance with PCI DSS.	40%
Q1b. My organization's CEO is a strong supporter of PCI DSS compliance efforts.	45%
Q1c. My organization views data security as a strategic initiative across the enterprise.	29%
Q1d. My organization is proactive in managing privacy and data protection risks.	48%
Q1e. Compliance with PCI DSS improves our organization's data security.	44%
Average	41%

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

Q3. Does your organization have security procedures and standards that are updated annually (or more frequently as deemed necessary)?	Pct%
Yes	35%
Yes, but not updated annually	26%
No	39%
Total	100%

Q4. Who in your organization is <u>most responsible</u> for ensuring compliance with PCI DSS requirements? Please select one response.	Pct%
No one person	21%
CIO	19%
CTO	8%
IT security leader (CISO)	23%
Privacy officer or leader (CPO)	2%
IT compliance	9%
Internal audit	2%
Legal	15%
Other (please specify)	1%
Total	100%

Q5. Who in your organization is involved in ensuring compliance with PCI DSS requirements? Please select all that apply.	Pct%
No one person	21%
CIO	59%
CTO	14%
IT security leader (CISO)	34%
Privacy officer or leader (CPO)	16%
IT compliance	19%
Internal audit	23%
Legal	37%
Other (please specify)	2%
Total	225%

Q6. Please select all the technologies in your organization that enable compliance with PCI DSS requirements. Then, for each item selected, 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.

Enabling technologies	Yes%	High	Moderate	Low
Access governance systems	55%	64%	24%	12%
Anti-virus & anti-malware solution	73%	74%	26%	0%
Code review	58%	36%	55%	9%
Correlation or event management systems	31%	55%	40%	5%
Data loss prevention systems	28%	43%	44%	14%
Database scanning and monitoring	42%	18%	33%	49%
Encryption for data at rest	65%	74%	14%	12%
Encryption for data in motion	64%	71%	18%	11%
Endpoint encryption solution	40%	46%	44%	10%
Firewalls	93%	82%	5%	13%
ID & credentialing system	27%	11%	37%	53%
Identity & access management systems	50%	63%	24%	13%
Intrusion detection or prevention systems	37%	22%	53%	25%
Perimeter or location surveillance systems	33%	3%	48%	49%
Traffic intelligence systems	13%	32%	31%	37%
Virtual privacy network (VPN)	40%	26%	62%	12%
Web application firewalls (WAF)	44%	55%	41%	4%
Website sniffer or crawlers	9%	7%	49%	44%
Average	45%	43%	36%	21%

Q7. Is your organization compliant with PCI DSS requirements today?	Pct%
Yes, for all applications and databases across the enterprise	22%
Yes, for most applications and databases across the enterprise	28%
Yes, but only for some applications and databases across the enterprise	25%
No	25%
Total	

Q8. What statement best describes your organization's scope of PCI DSS compliance?	Pct%
Our PCI DSS efforts are focused solely on the protection of cardholder data.	55%
Our PCI DSS efforts include cardholder data plus other sensitive consumer information such as Social Security Numbers, driver's license numbers, bank account details and so forth.	33%
Our PCI DSS efforts include all data about people and families	12%
None of the above	0%
Total	100%

Q9a. Did your organization experience a data breach involving the lost or theft of credit card information?	Pct%
Yes, only one incident	38%
Yes, two to five incidents	30%
Yes, more than five incidents	11%
No	21%
Total	100%

Q9b. If you said yes, did you publicly disclose the data breach?	Pct%
Yes, for all data breach incidents experienced	20%
Yes, for some data breach incidents experienced	44%
No, disclosure was not necessary	36%
Total	100%

Q10. The following matrix lists 10 common threats to the data security environment. Does PCI DSS decrease, have no impact or increase each security threat?	PCI decreases threat	PCI has no impact on threat	PCI increases threat
Loss or theft of confidential or sensitive information	51%	47%	2%
Economic espionage	12%	86%	2%
Social engineering	40%	47%	13%
Malicious employee attacks	50%	49%	1%
Cyber security attacks	41%	58%	0%
Surreptitious downloads of malware, virus, worm or Trojan that penetrates your company's network or enterprise system	34%	66%	0%
Use of insecure cloud computing applications or platform	17%	81%	2%
Policies and procedures are not monitored or enforced	59%	10%	31%
Insecure endpoints connect to the network or enterprise system	49%	50%	1%
Denial of service attacks	32%	67%	1%
Average	39%	56%	5%

Q11. With respect to the above list of threats to data security, where are the most serious threats located? Please select only two top choices.	Pct%
Wireless devices	38%
Endpoints	50%
Networks	22%
Applications	28%
Databases	15%
Off-line data-bearing devices	11%
Paper documents	29%
Total	193%

Q12. The following matrix lists 25 attributes that define the IT security environment. How has PCI DSS strengthened, had no impact or weakened each security attribute?	PCI DSS strengthened	PCI DSS has no impact	PCI DSS weakened
Identify major data breaches involving sensitive or confidential information	44%	52%	4%
Determine the root causes of major data breaches involving sensitive or confidential information	28%	69%	3%
Know where sensitive or confidential information is physically located	47%	50%	4%
Secure sensitive or confidential data at rest	54%	44%	2%
Secure sensitive or confidential data in motion	55%	42%	2%
Secure endpoints to the network	39%	57%	4%
Identify system end-users before granting access to sensitive or confidential information	31%	65%	3%
Protect sensitive or confidential information used by outsourcers (including third-parties, affiliates, and business partners)	11%	69%	20%
Prevent or curtail major data breaches involving sensitive or confidential information	18%	76%	6%
Prevent or curtail hacking attempts to acquire sensitive or confidential information	14%	76%	9%
Limit physical access to data storage devices containing sensitive or confidential information	40%	58%	2%
Demonstrate the economic value or other tangible benefits of the company's IT security program	61%	30%	9%
Ensure minimal downtime or disruptions to systems resulting from security problems	18%	79%	3%
Comply with legal requirements and policies (including privacy laws and statutes)	61%	32%	8%
Confirm with other regulatory requirements such as HIPAA, ISO and others	25%	74%	0%
Prevent or curtail viruses, worms, Trojans and spyware infections	39%	60%	1%
Perform timely updates for all major security patches	33%	60%	7%
Control all live data used in systems development activities	35%	63%	2%
Enforce corporate policies, including the termination of employees or contractors who pose a serious insider threat	45%	50%	5%

Attract and retain high quality IT security personnel	48%	50%	2%
Training and awareness program for all system users	51%	47%	2%
Conduct independent audits of the system	53%	41%	6%
Manage security programs consistently	66%	33%	0%
Prevent or curtail denial of service attacks	19%	78%	3%
Manage encryption keys	31%	70%	0%
Average	39%	57%	4%

Q13. Approximately, what dollar range best describes your organization's IT security budget in the present fiscal year?	Pct%	Median	Estimate
Less than \$1 million	5%	0.8	0.04
Between \$1 to 2 million	4%	1.5	0.06
Between \$3 to \$4 million	3%	3.5	0.11
Between \$5 to \$6 million	7%	5.5	0.41
Between \$7 to \$8 million	7%	7.5	0.51
Between \$9 to \$10 million	3%	9.5	0.24
Between \$11 to \$12 million	10%	11.5	1.14
Between \$13 to \$14 million	10%	13.5	1.30
Between \$15 to \$16 million	13%	15.5	1.94
Between \$17 to \$18 million	0%	17.5	-
Between \$19 to \$20 million	1%	19.5	0.26
Over \$20 million	38%	24	9.01
Total	100%		\$15.02
Point estimate	\$15.02		

Q14. Approximately, what percentage of the current IT security budget will go to achieving PCI DSS compliance?	Pct%	Median	Estimate
Less than 5%	4%	4.00%	0%
Between 5% to 10%	5%	7.50%	0%
Between 10% to 20%	8%	15.00%	1%
Between 20% to 30%	15%	25.00%	4%
Between 30% to 40%	32%	35.00%	11%
Between 40% to 50%	20%	45.00%	9%
Between 50% to 60%	7%	55.00%	4%
Between 60% to 70%	4%	65.00%	3%
Between 70% to 80%	0%	75.00%	0%
Between 80% to 90%	3%	85.00%	3%
Between 90% to 100%	0%	95.00%	0%
Total	100%		35%
Point estimate	35%		

Q15. Approximately, what percentage of the traditional IT security budget has shifted or been moved to PCI DSS compliance goals?	Pct%	Median	Estimate
Less than 5%	16%	4.00%	1%
Between 5% to 10%	8%	7.50%	1%
Between 10% to 20%	16%	15.00%	2%
Between 20% to 30%	17%	25.00%	4%
Between 30% to 40%	13%	35.00%	5%
Between 40% to 50%	5%	45.00%	2%
Between 50% to 60%	3%	55.00%	2%
Between 60% to 70%	2%	65.00%	1%
Between 70% to 80%	0%	75.00%	0%
Between 80% to 90%	3%	85.00%	3%
Between 90% to 100%	17%	95.00%	16%
Total	100%		36%
Point estimate	36%		

Q16. Please choose one statement that best describes the value of PCI DSS expenditures to your organization.	Pct%
PCI DSS compliance contributes more value than expenditures made.	23%
PCI DSS compliance contributes about the same value as expenditures made.	43%
PCI DSS compliance contributes less value than expenditures made.	34%
Total	100%

Q17. Please select the value PCI DSS compliance provides your organization. Check all that apply.	Pct%
Improves our organization's data security posture.	45%
Improves our organization's marketplace brand and reputation.	21%
Improves our organization's relationship with key business partners.	64%
Heightens awareness among C-levels within our organization.	33%
Helps secure more funding for IT security.	63%
Other (please specify)	0%
Total	226%

Q18. 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.	Pct%
Not necessary.	36%
Only "CYA."	33%
Necessary to achieve consistent security practices across the enterprise.	30%
Necessary to obtain buy-in from management.	47%
Necessary to secure security budget and funding.	52%
Necessary to prioritize security requirements.	46%
Essential to achieving an effective security posture.	48%
Total	291%

Organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	0%
Vice President	1%
Director	16%
Manager	36%
Technician	25%
Associate/Staff	4%
Other	18%
Total	100%

D2. Check the Primary Person you or your IT security leader reports to within the organization.	Pct%
Chief Financial Officer	4%
General Counsel	0%
Chief Information Officer	55%
Compliance Officer	3%
Chief Technology Officer	11%
Human Resources VP	3%
Chief Security Officer	14%
Chief Risk Officer	8%
Other	2%
Total	100%

D3. Total years of business experience	Mean
Total years of security experience	10.07
Total years in current position years	3.16

D4. Where are your employees located? (check all that apply):	Pct%
United States	100%
Canada	56%
Europe	45%
Asia-Pacific	34%
Latin America (including Mexico)	26%
Total	261%

D5. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	15%
500 to 1,000 people	19%
1,001 to 5,000 people	22%
5,001 to 25,000 people	20%
25,001 to 75,000 people	14%
More than 75,000 people	10%
Total	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

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.