



Payment Security and the SMB:

The Fifth Annual Survey of Level 4 Merchant PCI Compliance Trends

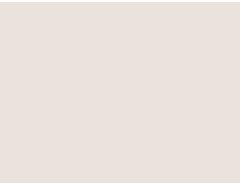
A Research Report
November 2013



Merchant Warehouse



Table of Contents:



	Page:
Executive Summary:.....	3
Methodology and Audience Profile:.....	4
Key Findings:	6
Detailed Findings and Commentary:.....	10
Recommendations for Merchant Service Providers:	22

Executive Summary:

It's time for a fresh perspective on payment security and the SMB.

Nothing in the American marketplace is more diverse than the Level 4 merchant group. Representing 98% of all U.S. retailers and primarily comprised of small to mid-sized businesses (SMBs), merchants in this card-brand-defined group number in the millions.

Businesses that fall within the Level 4 merchant group do, however, share important characteristics when it comes to securing the data they capture during the electronic (e.g., credit/debit) payment process. These commonalities are valuable to the entire payments chain—from credit card brands, to issuing banks, to merchant acquirers and the merchants they serve, and finally to cardholders.

Since 2009, ControlScan has conducted an annual survey to better measure and understand Level 4 merchants' challenges in understanding payment security best practices and complying with the Payment Card Industry Data Security Standard (PCI DSS). This year, in partnership with Merchant Warehouse, we once again approached the Level 4 merchant group, but with some new objectives.

The 2013 Survey of Level 4 Merchant PCI Compliance Trends retains core questions from previous surveys for continuity and trending purposes. Research questions supporting this objective include:

- Has anything changed with regard to Level 4 merchant PCI compliance awareness? Validation?
- To what degree are these merchants concerned about cybercriminal activity impacting their business? What about insider threats?
- Do they see value in the PCI compliance process? And do they connect it with the idea of reducing their business risk?
- What are these merchants specifically doing to secure sensitive information? What level of responsibility do they think they should have in securing cardholder data?

In addition to the above, the 2013 survey expands upon specific topics that are timely and relevant to the independent sales organizations (ISOs), acquirers and other merchant service providers (MSPs) working directly with Level 4 merchants:

- Does the length of time a merchant has been accepting credit/debit cards influence PCI awareness? Action?
- Are these merchants prepared for a data breach, should one occur? What are their attitudes concerning the impact a breach could have on their business?

- Do those who have purchased data breach insurance think it absolves them from security-related responsibilities and/or concerns?
- What level of importance are these merchants placing on security and compliance? How much time and money are they investing? What level of importance are they placing on service provider PCI compliance?
- Are Level 4 merchants looking to their MSP for technology solutions that can improve their security posture and make security simpler to maintain? What solutions are of interest and provide value?

This report answers all of these research questions, discussing the implications Level 4 merchants' responses have for the breach risk their businesses—and, consequently, the MSPs serving them—take on. We'll begin by reviewing the 2013 survey's methodology, audience profile and key findings, and then move into a detailed, question-by-question analysis followed by our recommended action steps for MSPs.

Level 4 merchants, as defined by Visa, are merchants processing fewer than 20,000 Visa ecommerce transactions annually. For brick-and-mortar and other retailers, Level 4 merchants are those that process up to 1 million Visa transactions annually.

Methodology and Audience Profile:

Conducted in September 2013, this year's survey was sent to randomly selected Level 4 merchants listed in the databases of two separate entities:

- ControlScan, which delivers payment security and compliance solutions to a global network of merchant service providers and the small businesses they serve, and
- Merchant Warehouse, a leading provider of payment technologies and merchant services, and one of the largest independent sales organizations (ISOs) in the credit card processing industry.

A total of 615 merchants completed all or a portion of the online survey. The population of responders has the following characteristics:

Audience profile by...	Percent of responses
Merchant type:	
Retail/brick-and-mortar.....	43%
Ecommerce	20%
Mail/telephone order, hybrids, and other.....	37%
Respondent's title/function:	
CEO, President, Owner	56%
Finance	17%
IT	15%
Manager or Supervisor.....	8%
Other.....	4%
Number of employees:	
1 to 10	58%
11 to 50	25%
51 or more.....	17%
Annual transaction volume:	
Under \$100,000	24%
\$101,000 to \$250,000	25%
\$251,000 to \$500,000	24%
Over \$500,000	27%
Annual sales volume:	
Under \$100,000	12%
\$101,000 to \$500,000	33%
\$501,000 to \$1,000,000	20%
Over \$1,000,000	35%
How long in business:	
Less than 2 years.....	5%
2 to 5 years.....	13%
More than 5 years.....	82%

Key Findings:

1. SMB merchants' PCI compliance awareness is growing, but significant payment security challenges remain.

With the majority (82%) of this year's survey respondents having been in business five years or more, they've clearly been around long enough to have at least heard of "PCI compliance." And, survey data indicate that merchants with at least some awareness of the PCI DSS are beginning to stand up and take notice:

- The percentage of merchants validating compliance grew substantially, from 50% in 2012 to 70% in 2013;
- At 40%, the number of merchants who agree that complying with the PCI DSS makes them "much more secure" is significantly higher than those who disagree (28%); and
- There has been a significant increase in merchants' understanding of why the PCI DSS applies to their business.

The above statistics are certainly encouraging, but there is more work to be done when it comes to Level 4 merchants' awareness and response to the payment security threats that plague their space:

- The vast majority (71%) continue to think they are at little-to-no risk for data compromise;
- Should a breach occur, 64% have no formal incident response plan in place and are therefore unprepared to quickly and properly address the situation;
- Nearly half (48%) have spent less than eight hours over the last year conducting compliance and security related activities; and
- More than one-third (36%) did nothing PCI related in the last year, with the exception of "completing the paperwork."

These and other findings indicate that many Level 4 merchants are either not understanding the full scope of their business's PCI compliance responsibility or they are of the "it can't happen to me" mindset—or possibly both. Merchant service providers should serve as trusted advisors in this area, conducting comprehensive, ongoing and targeted outreach communications that stir a dialogue and create action.

2. Formal responsibility for information security typically falls on the person who heads the organization, or no one at all.

Most SMBs struggle to successfully (and cost-effectively) balance the operational aspects of doing business; the smaller the business, the greater the struggle. In the Level 4 merchant segment, it can be difficult to establish a formal commitment to information security.

Survey data show that when it comes to payment security and the SMB, the balance of responsibility often shifts to the head of the organization:

- 43% of respondents say they are personally responsible for information security, two-thirds of which are the CEO/President/Owner, etc;
- 35% of respondents say no one is assigned responsibility—and for brick-and-mortar merchants, the number climbs to 45%; and
- Even in companies with 51 or more employees, 22% have no one assigned to information security.

This lack of focus on payment security places significant risk on the merchant:

- 51% do not require their third-party service providers to achieve and maintain PCI compliance;
- Only 36% have taken time to create an incident response plan (IRP) for their business and of those who have, less than half take the time to review and test it regularly; and
- Brick-and-mortar retailers are at the greatest risk, with 45% saying no one is formally responsible for overseeing security for their business.

In addition, the technologies and services most desired by these merchants represent “set it and forget it” style solutions, including anti-malware/anti-virus software, point-to-point encryption (P2PE) services, network firewalls and PCI-compliant hosting services. In other words, Level 4 merchants are looking to their MSP for technology solutions that can improve their security and make it simpler and less time consuming to maintain.

3. Merchants who are familiar with the PCI DSS and have 10 or fewer employees perceive—and receive—less value from compliance.

Survey-respondent demographic segmentation reveals a line of demarcation between Level 4 merchants with 10 or fewer employees and those with higher employee counts. This division is reflected in PCI compliance related sentiment and progress.

Of merchants with few or no employees who are also at least “somewhat familiar” with the PCI DSS:

- 38% don’t think the standard is helping make their business more secure;
- 36% of those who haven’t validated compliance say it’s “not a priority”; and
- 72% are not prepared should a breach occur (46% don’t have an IRP and an additional 26% admit they don’t even know what an IRP is).

In addition, this group is spending less money and time on the PCI compliance process than other Level 4 merchants, and 44% who validated compliance say they did nothing but “complete the paperwork.” Well-off-average responses such as these could suggest that these merchants are more apathetic and given to checkbox compliance.

Free-form comments from merchants with 10 or fewer employees also support the above conclusion:

- “Not sure it does apply to my business. My POS and merchant services are in that line of business [and] they keep it solid.”
- “Only issue is customer credit card security, and POS plus [payment processor name] do that.”
- “Small business run by owners.”
- “We are already covered under HIPAA.”

In general, these merchants are doing less to secure cardholder data, claiming a lower level of responsibility than their Level 4 counterparts. This reduced focus on payment data security, coupled with high transaction volumes, can translate to a greater risk of breach.¹

¹. Source: Symantec 2013 Internet Security Threat Report
(http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf).

4. High-transaction, Level 4 merchants are operating at higher risk—and many don't even know it.

The PCI DSS applies to any business accepting, transmitting or storing cardholder data. The standard is the same, regardless the number of credit/debit payments the merchant accepts within a year's time. While even the smallest business falls under this requirement should they accept just one electronic payment, the odds that a business will be breached increase as the number of transactions it accepts (e.g., its transaction level) increases.

The 250,000 transaction level serves as a mid-point that roughly divides the base of respondents into two halves. With that in mind, the following is true of Level 4 merchants with 251,000 annual transactions and higher:

- More than one-quarter (27%) are “not at all” familiar with the PCI DSS;
- One-third (33%) haven't completed their PCI compliance validation because it's “not a priority”; and
- They are just as likely as their counterparts to have “no one” formally assigned to manage payment security and compliance for their organization.

In addition, 48% of high-transaction, Level 4 merchants spent less than eight hours achieving and maintaining PCI compliance in the last year, and the same percentage (48%) say they spent less than \$500 on the activity. This makes sense, when 34% reveal they did nothing but “complete the paperwork.”

The above findings show a lack of engagement with the PCI DSS, but a deeper look into the higher-transaction merchant responses reveals a strong awareness and belief in the standard's objectives:

- 79% believe the PCI DSS should apply to their business;
- 52% place a high priority on the PCI compliance status of their third-party service providers; and
- 43% agree that compliance with the PCI DSS makes their business “much more secure.”

MSPs should pay close attention to this higher-transaction segment of their Level 4 merchant portfolio. These merchants are “bought in” to the PCI DSS; they just need to be further educated on their risk level and associated responsibilities.

Detailed Findings and Commentary:

1. In your opinion, how big of a risk does your company face from a data compromise?

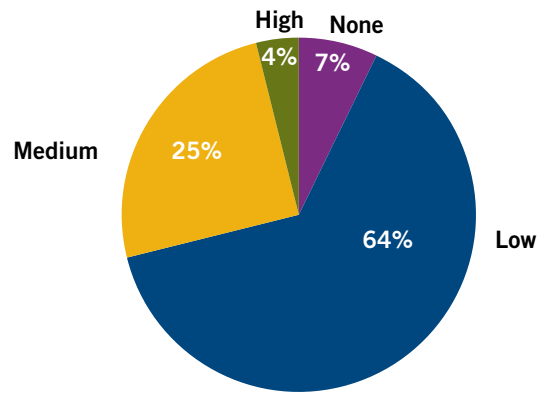


figure 1

RESPONDENT'S COMMENT

"I don't store credit card information."

As in previous years, the vast majority of respondents (71%) still consider themselves to be at little to no risk of data compromise. The good news is that year over year data show a slight downward trend in this number: Last year, the "little to no risk" percentage was 79% and in 2011 it was 82%.

As evidenced in other responses to this year's survey, a sober awareness of electronic payment risks can create a greater sense of respect for payment security and PCI compliance.

2. Has your company ever experienced a data breach?

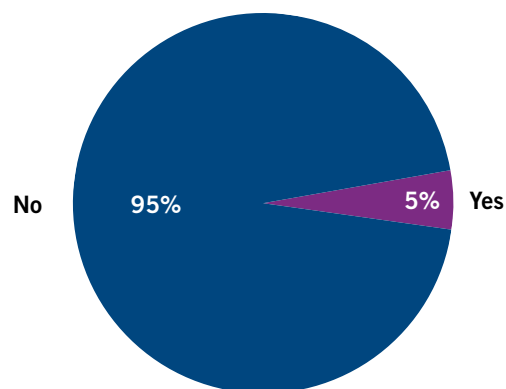


figure 2

This question typically elicits a small response percentage that answers "yes"; however, 5% of this year's respondents did indicate they had suffered a data breach. In fact, Level 4 merchants of all sizes were represented in that 5%.

When asked about the breach's impact to their business (a new question within this year's survey), 50% indicated it was medium or high, with "high" meaning that it nearly put them out of business. Interestingly, merchants in the "11 to 50 employees" range reported a greater impact than their smaller and larger counterparts.

3. If your business were to experience a data breach, what do you think the impact would be in terms of...

...fines, fees and other direct financial losses?

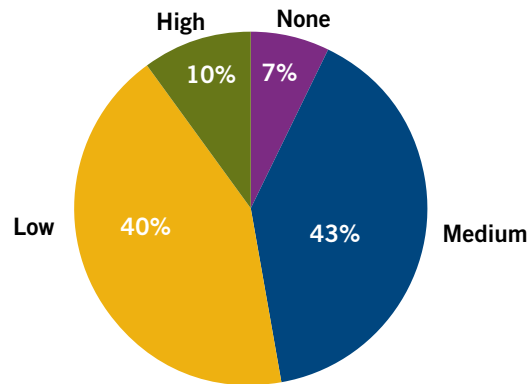


figure 3A

...lost revenue from weakened brand image?

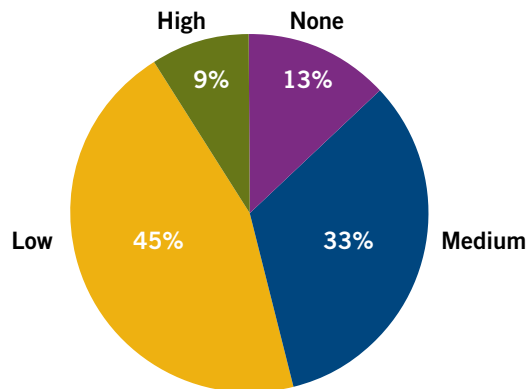


figure 3B

As figure 3A shows, slightly more than half (53%) of respondents think a data breach represents a medium to high financial risk for their business. Fewer respondents are concerned about a breach's impact to their brand image, as shown in figure 3B. However, a notable trend appears when the responses are analyzed according to number of employees: The larger the Level 4 merchant, the greater the importance placed upon a breach's financial and brand risk to the merchant.

4. Which of the following breach scenarios do you think is the greatest threat to your business?

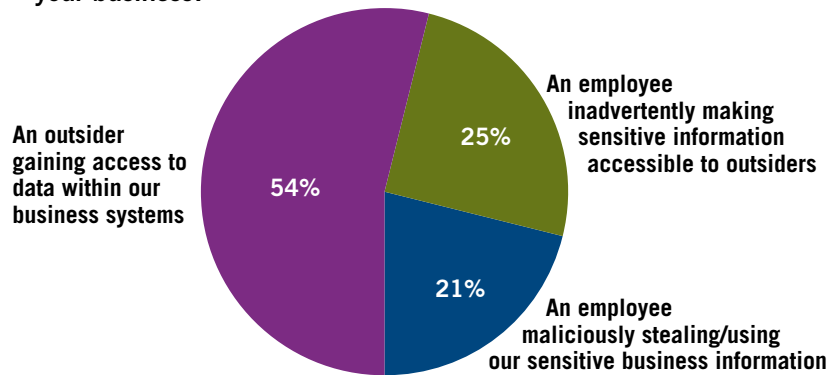


figure 4

In previous years' surveys, we asked respondents to simply differentiate between internal (e.g., employee) and external (e.g., hacker or criminal) threats. This year we provided three answer choices to better gauge threat awareness: 1) An outsider gaining access through malicious intent, 2) An employee maliciously using or stealing sensitive business information, and 3) An employee inadvertently making sensitive information available to outsiders.

While the majority of respondents still say outsider threats are their greater concern, there is less of a gap between insiders and outsiders than in previous years. As can be expected, a look at company size reveals that larger organizations are more concerned about malicious insiders. Retailers, however, are slightly more concerned with an insider inadvertently giving access to an external hacker or criminal. This shows a greater need for security awareness training among frontline retail associates.

RESPONDENT'S COMMENT

"Thieves will get through any system. Like a lock on a door. You need it but it won't stop everyone."

5. Does your business have data breach insurance coverage?

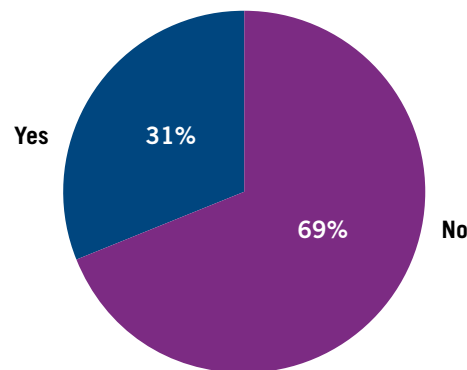


figure 5

The overall survey results show that less than one-third (31%) of Level 4 merchants have data breach insurance. Survey data also show that as an organization grows it is more apt to have breach insurance coverage; only 23% of organizations with 10 or fewer employees have breach insurance, while 60% of organizations with 51 or more employees have it. While it won't protect an organization from suffering a breach, data breach insurance coverage helps breach victims mitigate the financial impact of a breach by helping to cover contractual expenses such as forensic audit fees, card replacement costs and card-brand fines.

Breach insurance is a simple, low-cost way to help protect a merchant's business; however, merchants who have it shouldn't think it absolves them from security-related responsibilities and/or concerns.

Based on the findings from this survey, it is reasonable to conclude that the adopting merchants are taking a more holistic approach to data security. For example, 45% of survey respondents who have breach insurance also said a breach would have low-or-no financial impact to their business, and this percentage is consistent with the overall group average of 47% (Question 3A). In addition, only 23% say no one is responsible for the security of their business, which is well below the 35% overall average (Question 8).

6. Does your business have an incident response plan (IRP) in place?

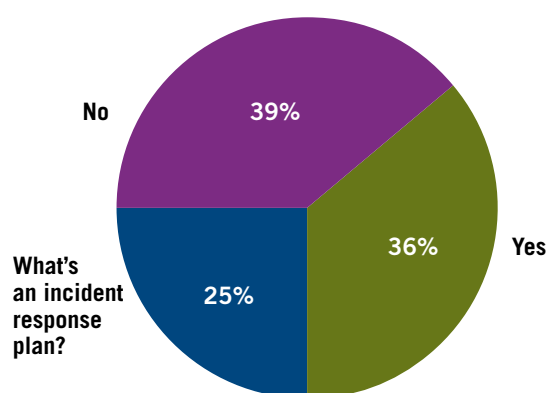


figure 6

While taking the proper steps to ensure payment data security is of paramount importance, a formally-documented, well-tested incident response plan (IRP) is also a must have, should a real or suspected breach incident take place.

Thirty-nine percent of survey respondents don't have an IRP in place, and an additional 25% admit they don't know what an IRP is. Even a sole proprietorship can benefit from an IRP, but this tool is mission critical for organizations with employees. Of the companies with 51 or more employees, 29% do not have an IRP in place and many of the respondents from these companies—including two IT professionals—have never heard of an "incident response plan."

7. [If the response to Question 6 was Yes]: Have you ever had to use your incident response plan?

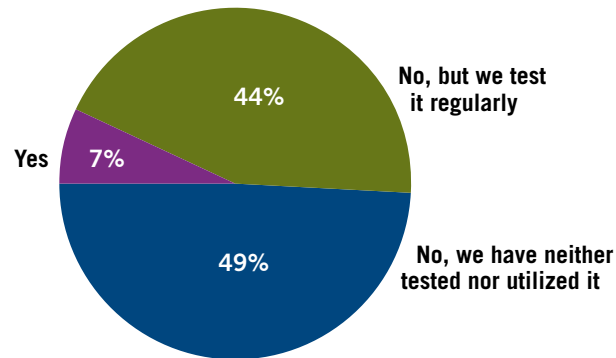


figure 7

The goal of this survey question was to understand the depth to which the 36% of respondents with an IRP have used their plan. Only 7% had to use their plan in what would be assumed a “real world” situation, while an additional 44% say they haven’t used it, but test it regularly.

8. Have you or another person been formally assigned responsibility for data security?

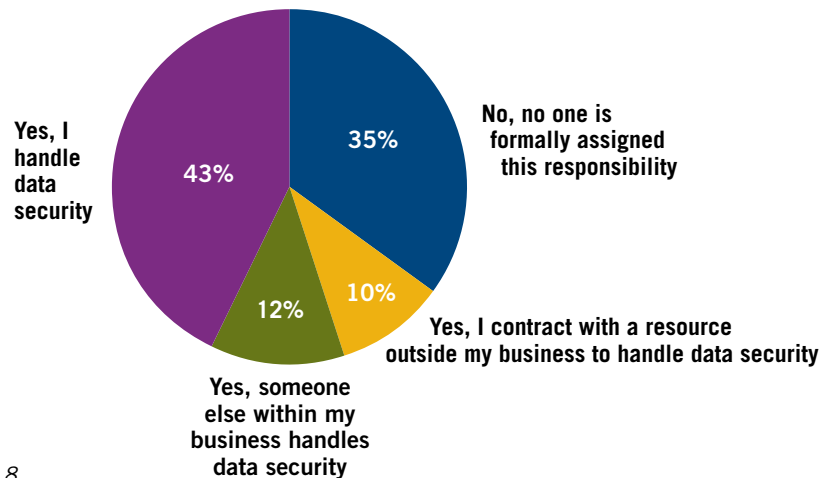


figure 8

RESPONDENT’S COMMENT

“Not worth the time and effort to spend so much time when you have so many other issues to tackle.”

As discussed in the Key Findings section of this research report, Level 4 merchants typically do not have a security expert to rely upon. In fact, most of these merchants are “going it alone” when it comes to payment security and compliance. And, those who have in-house or contract IT staff may think they are covered from a security standpoint, but many IT professionals are not aware of the steps the organization must take with regard to PCI compliance.

Overall, 35% of respondents don’t have anyone formally assigned to oversee their business’s data security. Twenty percent of these merchants say they are “just completing the paperwork,” while free-form responses indicate that many believe they should not be responsible for this aspect of doing business.

9. Are you familiar with the Payment Card Industry Data Security Standard (PCI DSS)?

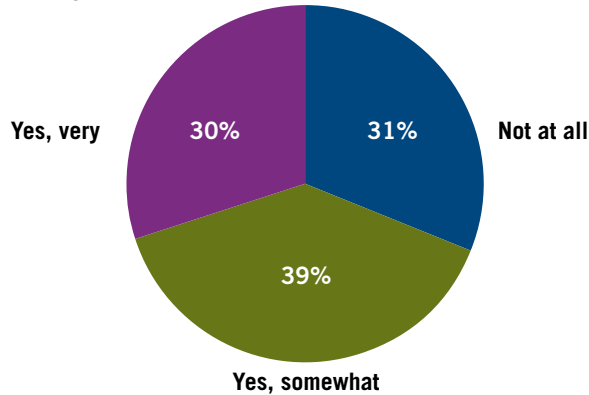


figure 9

This year a greater majority of respondents (69%) say they are at least “somewhat familiar” with the PCI DSS. While this is an encouraging increase over last year’s 54%, there are still concerns presented by corresponding survey data. For example, more than a quarter (27%) of respondents from companies with larger transaction volumes are “not at all familiar” with the PCI DSS; this lack of awareness, coupled with high activity, puts these organizations at high financial risk should a breach occur.

The remaining survey questions were completed by only those with some familiarity of the PCI DSS.

10. To whom do you consult to learn about data security and PCI compliance?
Check all that apply.

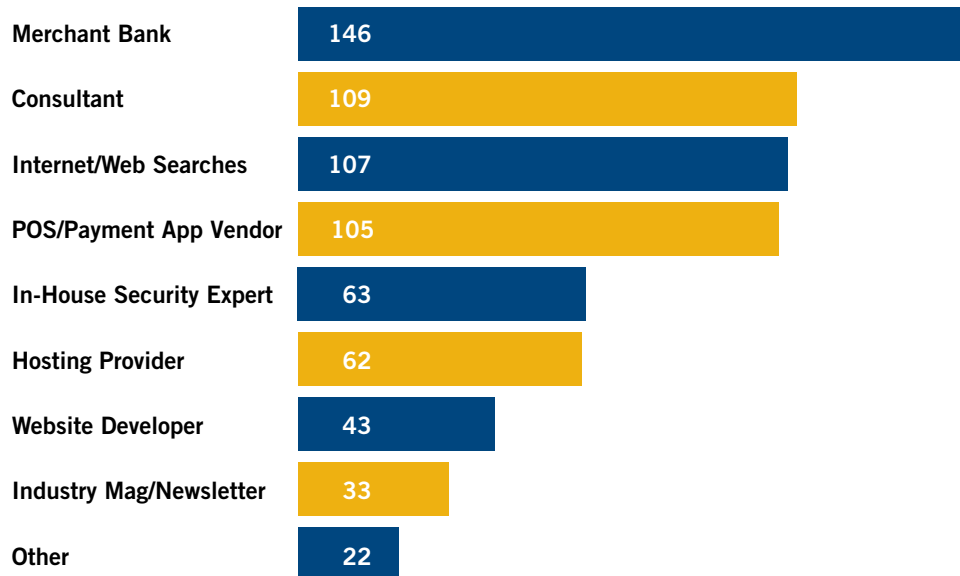


figure 10

The vast majority of Level 4 merchants continue to rely on their merchant bank for education about securing their customers' payment information. In addition, larger companies will reach out to consultants while ecommerce merchants will be more apt to conduct Web searches for more information.

11. Have you completed your annual PCI compliance validation?

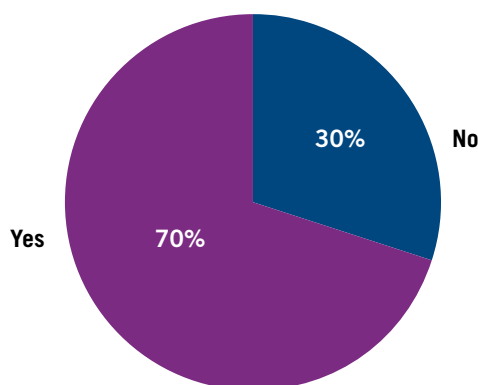


figure 11

RESPONDENT'S COMMENT

"I have mixed feelings about this. I do believe security is important, but I feel that PCI DSS was designed to offload issuing banks' risk of doing business to merchants."

This year, an encouraging 70% say they've completed their annual PCI compliance validation. As in previous years, brick-and-mortar retailers fall below the group average and ecommerce merchants are well above the average at 78%. When all 615 survey respondents are included in the calculation, the overall PCI compliance rate for these Level 4 merchants drops to 40%.

The PCI compliance validation process is meant to serve as a valuable tool for Level 4 merchants to assess their security posture and remediate any areas where their business does not meet the minimum bar set by the Data Security Standard. Merchants that do not participate in this annual process are most likely not staying in step with payment security best practices, making them more susceptible to breach. (Ninety-six percent of the breach victims Verizon studied for its 2012 Data Breach Investigations Report² were not PCI compliant at the time of the breach.)

². Source: Verizon 2012 Data Breach Investigations Report
(http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)

12. [If the response to Question 11 was No]: Why haven't you completed the PCI compliance process? Check all that apply.

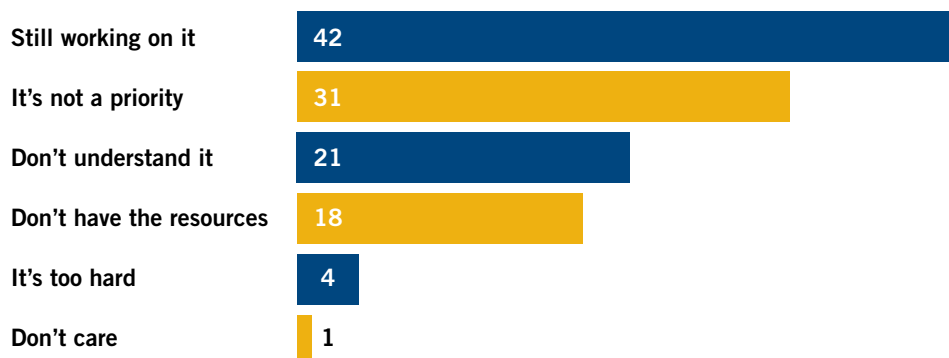


figure 12

Of those respondents who haven't yet completed their PCI compliance validation, "still working on it" is the primary reason given followed by "it isn't a priority." Brick-and-mortar retailers and businesses with ten or fewer employees were more likely to have assigned a low priority to PCI compliance validation.

13. In the course of the last year, what did you have to do or purchase in order to achieve and maintain PCI compliance? Check all that apply.

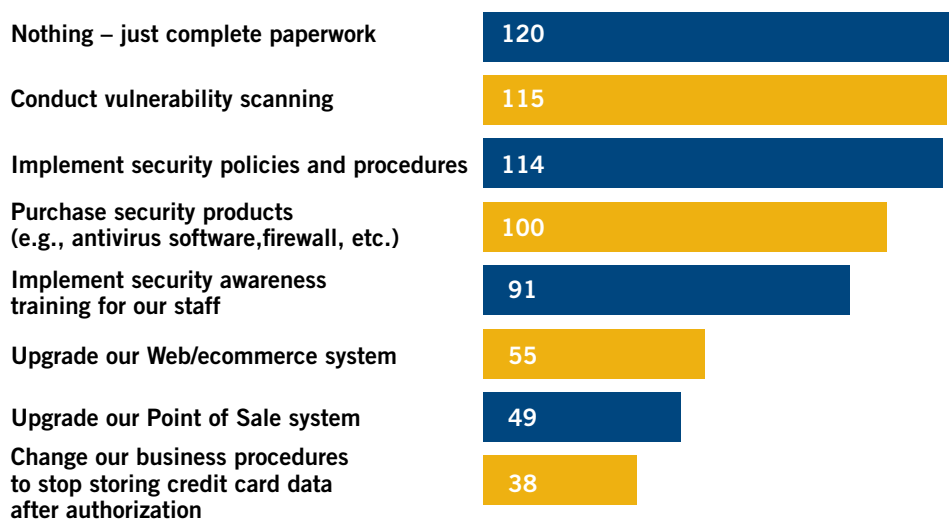


figure 13

The majority of Level 4 merchants continue to "just complete the paperwork" when it comes to compliance related activities. This year, 36% of overall respondents and 39% of retailers selected this option. In addition, one in three respondents from businesses with large transaction volumes (e.g., more than 250,000 transactions annually) do nothing to achieve or maintain compliance other than complete the paperwork.

Of the respondents selecting another option, vulnerability scanning was the most cited activity. It is important to keep in mind, however, that achieving and maintaining PCI compliance involves a number of different areas of activity and scanning is only one of them.

14. In the course of the last year, how much *time* have you and/or other company employees invested in achieving and maintaining PCI compliance?

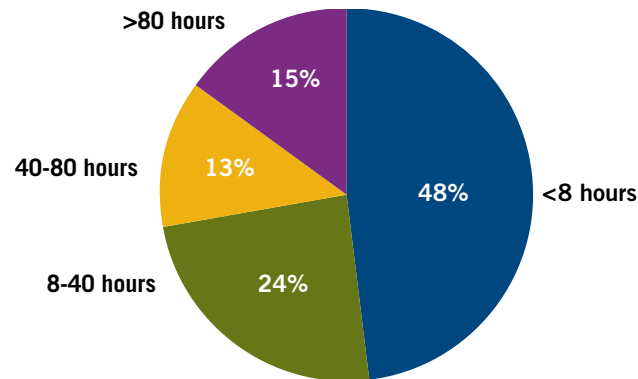


figure 14

Over a year's time, nearly half (48%) of Level 4 merchants are spending less than 8 hours total conducting PCI compliance related activities. Once again, businesses in the retail space are spending less time than the overall group. In addition, response data show that the smaller the business (in terms of employee size), the less time is spent. Transaction volume does not appear to influence the amount of time spent achieving or maintaining PCI compliance.

15. In the course of the last year, how much *money* has your business spent to achieve and maintain PCI compliance?

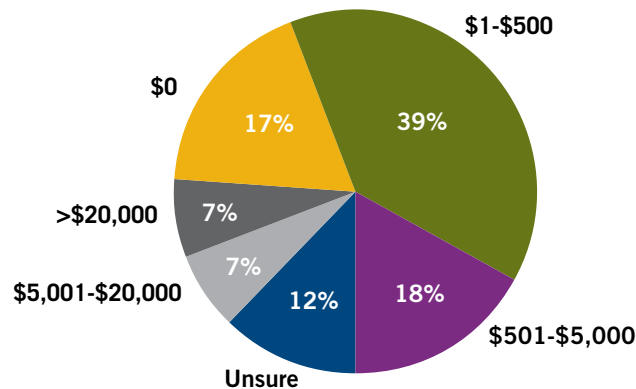


figure 15

RESPONDENT'S COMMENT

"Just adds another cost. Not sure being PCI compliant has changed anything."

Responses to this question are consistent with the time-based responses; retailers and smaller-sized businesses report below-average spending on PCI compliance related activities. Unlike the temporal component, however, businesses with higher transaction levels do tend to spend more money to achieve and maintain compliance. According to this year's survey, 20% of businesses with an annual transaction volume greater than 250,000 spent more than \$5,000. By contrast, only 7% of businesses with a lower transaction volume spent that amount.

16. Do you believe that complying with the PCI standard will help your business become more secure?

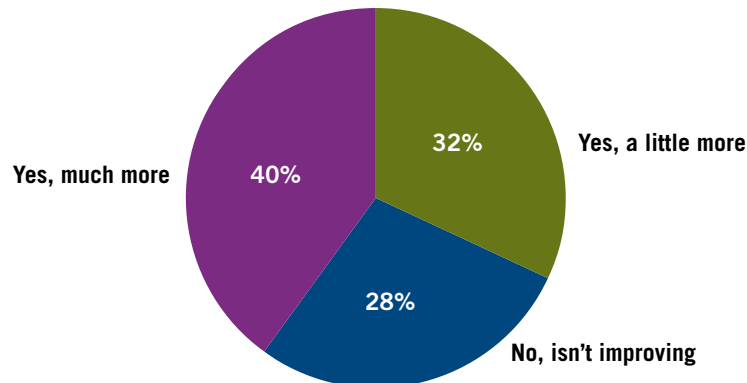


figure 16

RESPONDENT'S COMMENT

"It keeps customer information secure. It's nice to have a standard."

As a group, Level 4 merchants consistently agree that the PCI DSS is good for the security of their business. In fact, this year's percentage of merchants who agree that PCI makes them at least "a little more" secure is the highest it's been, at 72%. Free form responses convey a majority mindset that responsible businesses look out for the customer.

17. Do you think the PCI standard should apply to your business?

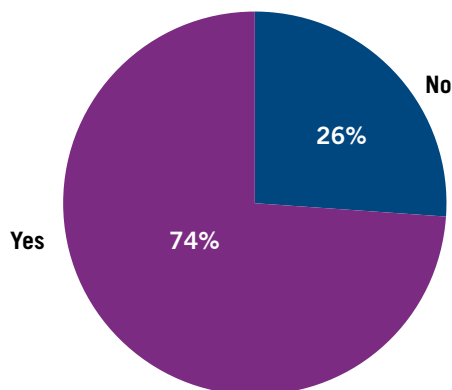


figure 17

RESPONDENT'S COMMENT

"Anyone handling cardholder data should be aware of how to handle it properly."

Again, the majority of respondents understand the need for the PCI DSS and its applicability to businesses accepting electronic forms of payment. At 74%, the "yes" response rate is once again the highest to date, perhaps reflecting a greater overall awareness of the benefits of the PCI DSS.

Many of those who don't believe the PCI standard should apply to them say they "don't store cardholder data" or that they're "too small to bother with," indicating they are missing the point of the standard. These respondents, who are typically (but not always) micro-merchants, also lack awareness of the threat landscape all merchants who accept credit and debit cards share.

18. How much importance do you place on the PCI compliance of your service providers and/or payment solutions?

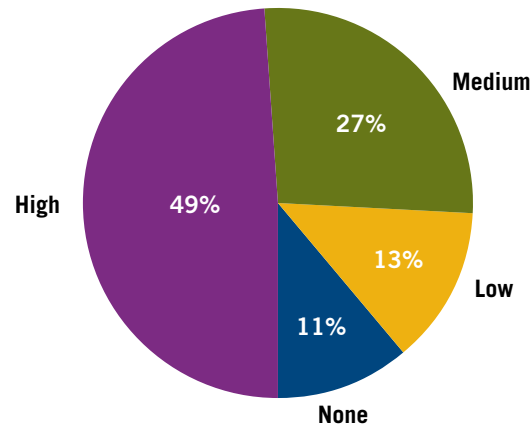


figure 18

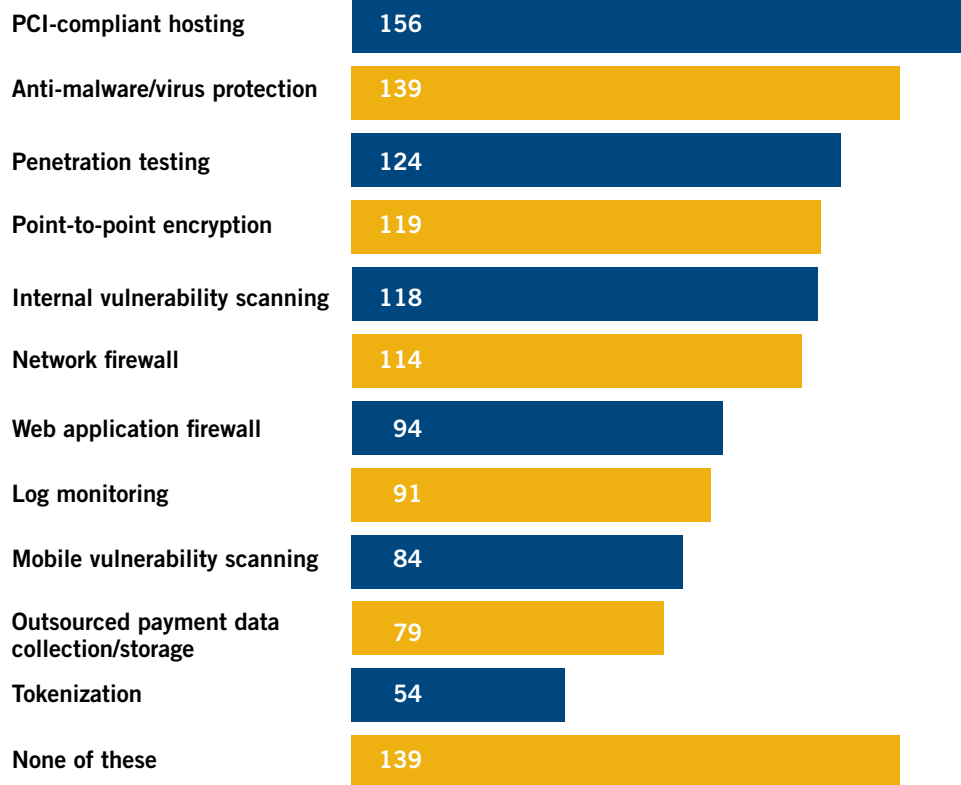
RESPONDENT'S COMMENT

"All businesses should do their part to secure customer data."

Third-party service providers are one of the most significant contributors to breach events, because their processes (or lack thereof) can impact the security of the merchant's cardholder data. First and foremost, it's critical that the merchant knows which of its service providers store, process or transmit cardholder data on their behalf. Many merchants are not aware of all the players involved and, as a result, have no idea if these providers are taking the right steps to protect their customers' data and ultimately their business.

As responses to this survey question also reveal, many merchants do not place an emphasis on third-party PCI compliance within the evaluation process. In fact, less than half (49%) require prospective service providers to prove compliance. Brick-and-mortar retailers are well below the group average, with only 43% saying third-party PCI compliance is a requirement for working with their business.

**19. What technologies and services could your merchant service provider(s) offer to help simplify the data security and compliance process for your business?
Select all that apply.**



RESPONDENT'S COMMENT

"Not really sure how all these technologies apply to us."

figure 19

Level 4 merchants want access to cost-effective technologies and services that can help simplify the data security and compliance process, but they don't have time to research and educate themselves on what's out there. This presents merchant service providers with a tremendous opportunity to differentiate themselves through proactive education and value-added business offerings that make the merchant's life easier while better securing their business.

MSP Recommendation: Motivate merchants by speaking their language.

Today, more Level 4 merchants have at least some awareness of the PCI DSS; however, many seem to be unsure of the steps they should be taking to effectively comply with the standard and better secure their business. In addition, free form comments reveal an underlying negative perception and distrust of the motives behind PCI compliance requirements:

- “More regulation, more headache and fees.”
- “PCI is about moving risk from banks to merchants so the banks can have higher margins.
- “The PCI standard is not specific and subject to interpretation.”
- “We already practiced security standards before PCI compliance was mandated.”

While SMB merchants may push back on conversations surrounding PCI compliance related activities, it doesn't necessarily indicate that they don't care about securing their customers' cardholder data. In fact, the overall sentiment expressed by the respondents to our survey is resoundingly positive.

MSPs can motivate merchants by speaking their language. In other words, it's time to change the conversation from a “PCI” focus to that of “security.” With protecting customers' data at the heart of the conversation, merchants will be more receptive to understanding the responsibility they have to put security best practices in place. Compliance then serves as a “check up” to see how well the merchant is doing in implementing its security practices.

Merchants focus on selling, not complying with standards

The merchant's primary concern is always going to be attracting customers and satisfying their needs, but certain points in the merchant lifecycle can lend themselves well to a security dialogue, including times at which the merchant is naturally changing or upgrading the way they process payments (e.g., their POS system and other pieces of their card data environment).

The onboarding and upgrade processes each present an ideal opportunity for MSPs to help merchants better understand their card processing environment and the flow of cardholder data during the payment transaction. These are also good times to review the merchant's third-party service providers and document the contact information in a central location. Furthermore, the MSP should ensure that its merchants clearly understand how a third-party provider's non-compliance with the PCI DSS could negatively impact their business.

The November 2013 release of PCI DSS version 3.0 is another milestone MSPs can leverage for merchant discussion. With this release, the Security Standards Council (SSC) has brought more clarity to the connection between data security and PCI guidelines. In addition, a concerted effort has been made to align the requirement updates with current breach trends. For example, the guidelines for Web application testing are now more specific with regard to assessing the security of the software as it relates to current and emerging threats.

Merchants want to operate cost effectively

Tight cost controls are a business reality for most if not all Level 4 merchants. This doesn't necessarily mean these merchants are adverse to value-added services; rather, it means that they are seeking a quick return on any technology or service they invest in on behalf of the business. Data security ROI is often not reflected in a revenue increase or other visible financial return, yet the MSP can create value for the merchant by demonstrating how reduced PCI scope can in turn reduce the merchant's PCI-related fees and curtail unnecessary technology spends.

Portfolio analysis can be highly useful to the MSP, because it helps with segmentation and helps frame merchant conversations according to the level of risk. Operational processes differ from business to business according to factors such as Merchant Category Classification (MCC), transaction volume, business versus consumer orientation, and more. By properly segmenting their merchant portfolio(s), the MSP can identify the merchants who, based on their cost-to-risk ratio, will most benefit from scope-reducing technologies.

Merchants need their MSP's input

Each year we ask Level 4 merchants to tell us who they are looking to for information and education on payment security and PCI compliance. Each year since the inaugural survey in 2009, respondents have consistently chosen "merchant bank" as their number one go-to resource. This year, Internet searches and consultants also came up high in merchants' selections.

As the merchant's payment enabler, the MSP is integral to the merchant's business success; they are, by their very nature, an ideal informational resource for the merchants they serve. MSPs who take the time to proactively learn and address their merchants' questions and needs will experience greater relational success.

The final question of this year's survey gave Level 4 merchants a list of security-related technologies and services they might find valuable to their business, should their MSP offer them. Respondents leaned toward offerings that would help them discover vulnerabilities (such as penetration testing) as well as those that would help them keep cybercriminals out of their business (e.g., PCI-compliant hosting, anti-malware/anti-virus software, firewalls, etc.).

Learning what merchants want begins with an understanding of their business concerns. If the idea of a potential data breach doesn't keep them up at night, then the MSP may want to foster a dialogue to create risk awareness and a corresponding sense of urgency. A number of respondents to our survey said they don't know anything about technologies or services that can simplify the data security and compliance process. Rather than signing a contract with a costly consultant or sifting through bits and pieces of information on the internet, these merchants would much rather engage with their merchant service provider.

About the Survey Sponsors:

ControlScan:

Headquartered in Atlanta, Georgia, ControlScan delivers payment security and compliance solutions to a global network of merchant service providers and the small businesses they serve. The company's innovative approach to secure hosted payment and PCI compliance solutions leverages technology, education and services to provide flexible options for its customers. Known for its thought leadership, ControlScan gives its customers a clear view of marketplace issues and trends so they can remain competitive. For more information, please visit www.controlscan.com, call 1-800-825-3301 or follow the company on Twitter at [@ControlScan](https://twitter.com/ControlScan).

Merchant Warehouse:

Merchant Warehouse is a leading provider of payment technologies and merchant services. The company's solutions enable merchants to more effectively connect and engage with their customers regardless of how, where or when they choose to shop. Merchant Warehouse's flagship technology solution, the Genius™ Customer Engagement Platform™, supports both traditional and new payment types, including mobile commerce, from a single countertop acceptance device.

Merchant Warehouse offers innovative payment solutions that help online and brick-and-mortar retailers, as well as point-of-sale (POS) developers, value-added resellers (VARs) and agents, strategically grow their business. Merchant Warehouse is one of the fastest growing payment technology companies in North America. For more information about Merchant Warehouse, please visit merchantwarehouse.com or follow the company on Twitter at [@MWarehouse](https://twitter.com/MWarehouse).