

## PCI by the Numbers: A Ponemon Institute Survey – an Interview with Dr. Larry Ponemon

Listen to Podcast [here](#).

**Brian Contos:** Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit [Imperva.com](http://Imperva.com), check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at [blog@imperva.com](mailto:blog@imperva.com).

Joining me today is Dr. Larry Ponemon. Dr. Ponemon is founder and chairman of the Ponemon Institute, a research think tank dedicated to advancing privacy and data protection practices.

Dr. Ponemon is considered a pioneer in privacy auditing and the Responsible Information Management or RIM framework. Dr. Ponemon consults with leading multinational organizations on global privacy management programs. He has extensive knowledge of regulatory frameworks for managing privacy and data security including financial services, healthcare, pharmaceutical, telecom and Internet.

Dr. Ponemon was appointed to the advisory committee for online apps security for the United States Federal Trade Commission. He was appointed by the White House to the Data Privacy and Integrity Advisory Committee for the Department of Homeland Security. And Dr. Ponemon was also appointed to two California State Taskforces on privacy and data security laws.

Dr. Ponemon is a member of the National Board of Advisors for the Eller College of Business and Public Administration at the University of Arizona. He serves as Chairman of the Government Policy Advisory Committee and Co-Chair of the Internet Task Force for the Council of American Survey and Research Organizations.

Dr. Ponemon earned his Ph.D. at Union College in New York. He has a Master's degree from Harvard University, and attended the doctoral program in system sciences at Carnegie Mellon University. Dr. Ponemon earned his Bachelor's with Highest Distinction from the University of Arizona. He is a Certified Public Accountant and a Certified Information Privacy Professional.

Dr. Ponemon is a Vietnam War era veteran of the United States Navy.

Well, welcome to the show Larry.

**Dr. Ponemon:** Thank you very much Brian, it's good to be here.

**Brian Contos:** So Larry, could you give our listeners a little bit of background on this recent PCI study that you've done?

**Dr. Ponemon:** Certainly, this study is about compliance with PCI DSS. Obviously you all know it's a major driver to security and to security compliance and lots of companies are spending some serious resources. We thought it would be important to do a reverse empirical study to find out if these organizations were in fact doing the right thing to get to PCI compliance. Maybe there were some gap areas and difficulties along the way and just in general to gauge their reaction.

If they achieve compliance, were they satisfied with the outcome, could it be done better in the future and could the program improve?

So we had lofty goals with the study and we are very, very pleased with the findings.

**Brian Contos:** What would you say are some of the top lessons learned from this survey?

**Dr. Ponemon:** Well there's a couple of I think very interesting findings and then we can translate that into lessons learned. I think the number one issue is that probably compliance... Good compliance is not exactly good security, that organizations maybe in a compliance state with PCI DSS but if they are not doing a whole bunch of other things, they might not be achieving the best... most appropriate security posture for the organizations, so I think that that's clear from the findings.

I also think that a fair number of organizations feel that the PCC DSS process was very helpful to them because, although it's a narrow set of issues, you know... cardholder data... a lot of organizations, and seem like the smarter organizations use PCI as an opportunity to improve other aspects of the company security posture.

You know PCI DSS as a compliance requirement, you have to do it and if you have the resource to do that maybe with just a little bit more resources and maybe being smart in the spending on those resources, you can accomplish more and better security.

I think we found that some organizations use PCI as an opportunity to do more and achieve better outcome for their company.

**Brian Contos:** I am not going to go into too many of the stats because certainly people can download the whitepaper and read through it and I think it will add more color being able to see it, but there's three specific statistics that I just want to sort of get your reaction to and how you would read that. The first one is 71% of respondent said that they don't treat data security as a strategic initiative even though 79% of them had already experienced a data breach.

Now that seems like a real interesting dichotomy just virtually the same amount say "Eh, we don't think that's strategic, but yeah we definitely had breaches and there's been issues."

How do you read that one?

**Dr. Ponemon:** Yeah it's really an interesting finding and maybe a little bit weird because you would think "OK, our company had a data breach, we'd better make security strategic otherwise we are going to lose our brand and reputation in the marketplace." But I am not sure that it occurs. I think in many organizations, there's almost an expectation that you'd never be perfect, so you are going to live with the consequences of data breach and therefore data breach notification as required by the various state laws...

## PCI DSS Survey Results with Larry Ponemon

That 71% is also very disturbing to me as well, because I think organizations need to view security and data protection and maybe privacy issues around cardholder information, which is customer information is absolutely strategic.

Failing to do that can get you into a lot of trouble, and ultimately you'll lose the confidence and trust of the cardholder or the customer. So it is surprising to me that 71% of the respondents say that their organizations do not treat data security as strategic.

**Brian Contos:** The second stat that I wanted to share, and when I first looked at, my gut reaction was "Wow, that's really low" but when I started thinking about this next stat, I really said to myself "Wow you know what, this is really the Holy Grail of regulations and compliance converging with security and that is... 27% of respondents said that they feel PCI compliance is perceived positively and contributes to an improved security posture.

So yet as first take, right around 30% doesn't seem like a big number but really this is what we've been preaching for years and the fact that 30% said that "Yeah you know, we are doing PCI compliance and it's actually helping with other initiatives." I actually think that's a pretty good stat.

What's your take on that one?

**Dr. Ponemon:** You know I have exactly the same reaction Brian. I looked at the number and said "Wait a second, you know, it's 27 or 30% of organizations believes that PCI improves their overall security posture, that seems pretty low" but then you think about it, a lot of organization sees PCI as a compliance thing only. So if you look at all of the organizations that potentially have to comply or should be complying with PCI, to say at 30% agree that their security posture improves suggest that PCI is pretty successful.

I think hats off to PCI, because that's a large number of companies that say this has been a very significant benefit to security.

**Brian Contos:** Yeah, I think if we did a similar study, this is just based off my own gut feeling on Sarbanes-Oxley or HIPAA or some of the EU laws, I think it would be much lower just because they are much more deterministic and they rely less on a prescriptive way of addressing the problem like PCI does. PCI is very very prescriptive in its approach, I think it gives people a roadmap if you will and they could actually leverage that where HIPAA, Sarbanes-Oxley to a certain extent is still kind of grey, still kind of fuzzy.

**Dr. Ponemon:** See I agree that the best way to measure - is this a big percentage, a small percentage, is it a positive and my gut is I think correct, I think it is, but I think if we have the exact same question and just inserted Sarbanes-Oxley, that percentage would be negligible probably in the single digit. So and I think you are right because PCI provides the detail that an organization needs, they'll look at HIPAA and God Bless HIPAA, because it doesn't actually give you the precise steps that you need to take and I think organizations like PCI, because it's so clearly defined...

They'd be missing some elements that basically is prescriptive... something that can be followed without too much difficulty.

**Brian Contos:** The last stat that I want to look at is 60% said they simply don't have the resources to address PCI and that seemed like a high number to me. Did you get any feeling if this is because they are not getting any executive level support or because they feel the cost to address PCI is just way too high to outweigh the business risk of fines?

What's driving this very large percentage?

**Dr. Ponemon:** Well 60% is a big number and basically we've done other studies of IT security and data protection and even privacy compliance programs. It seems that in general these issues... it seems like the endless abyss of spending... there's never enough resources available to get to security posture that is acceptable to a security expert like a CSO. And so I think... I am not saying these people are complaining and saying I need more resources and that's where we get the 60%, but I think it's pretty clear that resource constraints are a reality in this information security industry and to have 60% on this one is probably not a good fact but it's probably up.

That's just the reality of having limited resources to accomplish the security mission.

**Brian Contos:** You know I didn't think about it that way, I think you are absolutely right. If you would probably talk to anybody in the IT field, they'd probably never say "We have more than enough, we've got too many resources, take some away."

**Dr. Ponemon:** You know if they responded like too many resources or we have absolutely perfect amount of resource to get the job done, that means these people are smoking a strange cigarette. They are definitely not in the security industry, because it's a constant battle and whatever you fixed today, there will be other threats, other issues that will show up. And that's an issue at the C level, the C level doesn't understand, they feel like you've spent money on something, you're going to accomplish the mission and you are going to declare victory and end.

But this is a never ending cycle for lots of reasons.

**Brian Contos:** Can customers rely on companies to do the right thing when it comes to protecting the credit card information?

**Dr. Ponemon:** Well, you know I think the world has improved. I think that PCI has a lot to do with that improvement, to be honest with you and hats off to VISA for originating the VISA assist program. But I basically think that it's never going to be absolutely perfect, I think companies that achieve PCI are probably better but they are not perfect and we know that from places like Hartland and others.

But I think that over time the customers are going to hold companies, credit card companies, financial service organizations, merchants, online merchants and so forth to a higher standard and I think that's going to drive compliance rates as well.

And in fact one suggestion that we make in our paper is maybe some external seal that the consumers can read and so they can actually see the companies that are PCI compliant versus those that aren't and that might actually drive compliance to a higher state other than what we currently see today.

**Brian Contos:** Now and this pulls a little bit from the previous question on resources... are customers more at risk transacting with smaller companies because they might be more resource constrained and therefore maybe the companies can't do the due diligence to protect their credit card information?

**Dr. Ponemon:** Well, it's a depressing finding because you root for the underdog or the little company and we are a small company. I will safely say that when you are a small company, reality is limited resources. You are not going to have as many of the bells and whistles that even a medium size company or a larger company can afford to buy or spend.

## PCI DSS Survey Results with Larry Ponemon

So I think what we have here in this study is that smaller companies had a lower level of compliance with PCI DSS.

Probably not too surprising because it maybe had a different tier of compliance and so the date for compliance is a little bit later than tier ones or tier twos. But I basically think that smaller companies are more likely to have security vulnerability.

The only saving grace and it's probably not on the target list of the cyber criminals and places like Estonia and Russian Federation but those guys are pretty smart and that could be one way to gain entry right.

Just focus on the small company because small companies interact with large companies so I definitely think it's an issue but it doesn't mean stop buying from the small company. Small companies need your money and many small companies I'm sure are excellent around security.

But seems on average, larger companies are more likely to be in a better more reasonable state of compliance and achieve a higher security posture.

**Brian Contos:** Well there you mentioned budgets a little bit earlier. How PCI is affected security budgets? Has there been an explosion in budgets because of PCI?

**Dr. Ponemon:** Good question. And I think the evidence of the study suggests that, as defined by the IT and IT security practitioners in our study, one of the benefits was to get more funding, that PCI was one way to get funding for IT security. And in one question, we were able to extrapolate the percentage of IT security spent specifically and expressly on PCI. And it was about 30 to 35 percent, which we thought was pretty interesting.

So if you think about the IT security budget as maybe \$15 million, \$20 million for a company, and 35 percent on PCI, that's a pretty large percentage of the total, because, obviously, the security department or function is doing a lot of other things as well.

It was also interesting. We asked a second question on budget, and the question was not the direct spending on PCI but, basically, the moving of dollars from one category to another.

So you're actually incrementally not spending more, but basically moving budget to something that's viewed as more critical. And, again, PCI was viewed as the critical element that organizations were likely to shift funds to in order to achieve.

So if obtaining budget, like that 60-percent problem we talked about before, is an issue, clearly companies that are attempting to achieve compliance with PCI are more likely to have a higher budget, and maybe higher-level or seed-level support.

**Brian Contos:** So Larry, one of the things that I thought was very revealing in the survey, and it really boils down to a very simple statement: PCI is what you make it. How are companies approaching PCI? What's working? What's not working? Did you find any interesting details there?

**Dr. Ponemon:** Yeah, we asked questions. There was one, I'm not going to call it an anomaly, but it was a really weird finding, again, which was the kind of technologies that companies were implementing in order to achieve compliance. And we really tried to determine the effectiveness, or the cost-effectiveness, of these different technologies. And

## PCI DSS Survey Results with Larry Ponemon

what we found is that some organizations that were striving to become PCI-compliant were not actually implementing the appropriate technologies that are actually required under PCI.

So, for example, we didn't get 100 percent on firewalls. We said that a high percentage of companies had said that they were implementing firewalls, but it wasn't at 100 percent as required by PCI. Antivirus and anti-malware software, a very large percentage said that they were using it, but it wasn't at 100 percent.

So it seems that organizations might not necessarily be getting to compliance. I mean, maybe they're getting to a reasonable level of compliance, but they're not getting to the level of compliance, potentially, as envisioned by the PCI DSS folks. The standards require certain things to be in place.

And our results suggest that companies may be slightly below that level and still declaring victory: "We have compliance, even though we don't have a firewall in place."

That's not a good fact. I don't think there are many companies that fall into that category, but we don't have the level of technology implementation that we think is required under PCI. And there are other issues as well that suggest that companies may not be getting there, or they may not be getting there in the most efficient way.

**Brian Contos:** Well, Larry, as we wrap up here, I have one more question, and actually two statements before that. Whenever you talk about compliance, there's always two givens. One, nobody's ever in business to be compliant. You don't say, "I want to grow up and build the most compliant company in the world." And two is that compliance can be very expensive. The costs are high. How are smart companies able to lower that cost and really manage that and still achieve compliance?

**Dr. Ponemon:** Well, I think that there are some basic blocking and tackling steps that companies can take. And I'm not saying that it's costless to achieve compliance. I remember - just to deviate a little bit here - but there was something that was similar in the quality industry about 20 or 30 or 40 years ago. And there's a book called "Quality is Free." And the theory was that if you have perfect quality, say in the manufacturing process, you basically reduce your defects, and at the end of the day, guess what? You are basically paying zero dollars for better quality.

And I believe that to be true. It seems a little far-fetched at times, but I believe that to be true.

And I also think the same model applies, to some extent, to security, that if you do the basic things, you have the right tools and people are smart, and you do the right things in terms of managing data and keeping only the data that you need and being a good steward of the information and managing against privacy standards and all of these important issues.

If you do that right, you're going to reduce the risk of sloppy, incompetent, negligent employees, temporary employees or contractors. You just have to be consistent and mindful of the issue. You have to be a good manager of resources, because you're never going to have enough.

And you also have to think about the strategic consequences of what you do. Organizations that build a better governance framework for security usually achieve compliance with less resources. But I don't know if it's ever going to be security is free, because we do all of the things at the beginning, [laughs] the process-oriented things, really well.

## PCI DSS Survey Results with Larry Ponemon

I think there will always be a security risk that's costly, simply because we could never stay five or 10 steps ahead of the bad guys, the truly malicious cyber criminals that probably reside all over the world.

The key variable is that good companies, strategic companies, companies that take governance seriously are probably going to experience a lower cost than organizations that are purely tactical, have all sorts of problems. They're going to be spending the big bucks, and probably doing it with a consulting firm.

**Brian Contos:** Very well put, Larry. Extremely insightful as always, and it was a pleasure speaking with you. Thanks so much for joining us on today's podcast.

**Dr. Ponemon:** And thank you, Brian. It's a pleasure, and I look forward to talking with you soon.

**Brian Contos:** If you would like to learn more about this subject, and Imperva, please visit [imperva.com](http://imperva.com). For questions or comments about this podcast, please send email to [blog@imperva.com](mailto:blog@imperva.com). And follow us on Twitter for the latest Imperva news. **Brian Contos:** If you would like to learn more about this subject and Imperva, visit [imperva.com](http://imperva.com), check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at [blog@imperva.com](mailto:blog@imperva.com).



North America Headquarters  
3400 Bridge Parkway  
Suite 101  
Redwood Shores, CA 94065  
Tel: +1-650-345-9000  
Fax: +1-650-345-9004

International Headquarters  
125 Menachem Begin Street  
Tel Aviv 67010  
Israel  
Tel: +972-3-684-0100  
Fax: +972-3-684-0200