

## Web Application Security Survey & Analysis with Dr. Larry Ponemon

Listen to Podcasts: <http://www.imperva.com/resources/podcasts.asp>

**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 <http://www.imperva.com>, check out our blog at <http://blog.imperva.com>, follow us on Twitter at <http://www.twitter.com/imperva>, or send us an e-mail at [blog@imperva.com](mailto:blog@imperva.com).

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

Well, Larry, welcome back to the Imperva Podcast.

**Dr. Larry Ponemon:** Thank you very much, Brian. It's a pleasure to be here.

**Brian Contos:** So, Larry, like last time you were on the podcast, we were discussing a newly fleshed out research paper. But before we get into that, and some of the analysis there, please give our listening audience a little bit of background about the Ponemon Institute, and what exactly it is that you folks do there.

**Dr. Larry Ponemon:** Ponemon Institute is a research company studying privacy, data protection, and information security policy. The Ponemon Institute is in its 10th year, and we're very pleased to tell you that we are international. We do work in more than 50 countries. We continue to find it pretty enjoyable, even though research can be boring at times. We basically seem to choose research partners, like Imperva, that are interested in doing interesting and groundbreaking research, and that kind of motivates us.

**Brian Contos:** What exactly was this research based on? What types of things were you looking at?

**Dr. Larry Ponemon:** Well, the website risk, and web applications more generally, it's interesting. When you look at the data breaches that occur, say in the United States, the vast majority of data breaches are negligence, or incompetent employees, or even some system glitches. But the ones that fall into the category of malicious, criminal, seems to involve software violations to applications. And it's obviously happening at the website or through the Internet. So what we've wanted to do is understand how come so much of the risk that we see in information security is in and around websites. And we felt that it needed to be studied as its own area, because we've done other studies, of course, on different types of threats, and the changing threat landscape. But, specifically around websites and web applications, that's really the focus of this research.

**Brian Contos:** Great, so what are some of the glaring issues or maybe success points that you saw as a result of this analysis?

**Dr. Larry Ponemon:** Well, not too surprisingly, to an audience of learned IT and IT security practitioners, we basically learned that this is another area that we'll classify as a mess. Now, not to say, that across the boards, organizations are mismanaging their security responsibilities around websites. But it is clear that a lot of organizations have significant gaps. An example of a gap is we found, for example, 70 percent of the respondents in our study do not believe their organizations have sufficient resources to secure and protect critical website applications. 70 percent is a large number, and, obviously, you need resources in this business in order to get the job done.

Another example of a really big gap is about 33, 34 percent, one-third of respondents, admitted that they do not fix urgent vulnerabilities. Don't fix them. I'm not saying they take their time in fixing them, but they basically acknowledge that they're probably not being fixed. And, on average, developers spend about 18 hours to fix a single vulnerability.

So this is a problem. It's a time consuming problem. And it has a huge cost associated with the fixing of the vulnerability, or the not fixing of the vulnerability, which is the opportunity loss and all of the problems associated with an insecure website.

**Brian Contos:** Yeah, the vulnerabilities of websites, and web applications, and their corresponding databases together, it's very interesting when you start talking about fixing vulnerabilities there. I think a lot of people think of patch management from a personal perspective. You know, every Tuesday they update their Microsoft patches, and they click on something, and it slows down their system for a few minutes, and maybe reboots, and then they're good to go. But, on enterprise applications, especially these mission critical apps, there's a lot more to it than that, isn't there? There's QA to be done, and perhaps custom code needs to be written, or vendors actually have to generate and test new patches. It's a very complicated perspective, isn't it, when you're look at these mission critical apps?

**Dr. Larry Ponemon:** Oh, absolutely. I mean, you think you're doing your job when you're doing patch management, and you assume things are perfect in the patch. The fix is, the solution is, going to solve all of my problems. And then later you learn that that was going to create a whole bunch of new problems. Malicious code, of course, is one source of that monster. But it's just quality control issues, and lack of quality assurance, that creates a slew of vulnerabilities for organizations.

**Brian Contos:** Did you find that a lot of these organizations were or were not employing secure programming practices throughout; I guess we'll call it, the application life cycle? I mean, were they vetted, and writing secure code, or was it the afterthought? Or was it something that management didn't even feel was critical?

**Dr. Larry Ponemon:** What we basically found is that a lot of organizations didn't have a formal system for dealing with the life cycle issues and also a lack of accountability. It wasn't clear who in the organization was responsible. In other words, no one was responsible, because everyone thought it was the other guy that was actually taking care of the problems. So, for example, we found that website administrators, or information technology people, or people in the quality assurance, or IT compliance, or even IT operations, were touching some of the issue around security and trying to solve some of these issues. But it wasn't done in an integrated and holistic way. And I think probably is the source of a lot of the problems, and angst, that we saw in this study.

**Brian Contos:** So I guess the million dollar question is, at the core of this, why do you think applications, or more precisely application security, just seems like it's being

overlooked, it's being ignored? Is it resources? Is it education? What's really at the core of this?

**Dr. Larry Ponemon:** Well, there are a couple of theories here. And I think we have evidence to support the theory, at least in part. I think a lot of organizations, they spend around infrastructure and network, at that layer, and they basically aren't really looking at the application as a source of great risk. Although, I think the people in the trenches, the people who are dealing with security and rolling up their shirtsleeves, they see it. But at kind of the next level, or even at a higher level, like the CESA level, I think you're focusing on a whole bunch of things, and the application, web application, security issues has not actually risen to the level that it needs to be in order to get the attention that it needs. And we basically see that definitely in this paper.

I also think that it's hard. I mean, it's really hard to find, to do the debugging, and to find the bad code, so to speak. And that's why you have to rely on technologies like web application firewalls as the potential solution to the difficult... You know, it makes it a little easier, or maybe a lot easier. And then there may be some SSA-based solution that could actually help an organization, if they don't have the wherewithal in-house to fix the problem.

But it's an issue that hasn't risen to the top, and it probably will. And, number two, it does require resources that organizations don't necessarily have right now.

**Brian Contos:** Yeah, that's a good point. And I have a snippet of an early draft version of your report here with some really interesting stats. I'll just cover a few and then ask you for your feedback here. It says, secure coding requires resources we simply don't have. 70 percent of respondents felt that way. 56 percent said, developers simply aren't responsible for security. And about the same percent said, developers are just too busy to worry about security. It seems, fundamentally, these developers, and more so these organizations, it's, get the app out there, get it running, and get it operational. If it's revenue driven and helps drive revenue, or helps support some business operation then it's okay. But they don't seem to be incentivizing their developers or putting emphasis on their application vendors to actually provide them with secure stuff.

Make sure it's running, but hey, also make sure it's secure. It feels like there's a big gap there. It seems like we've almost gotten over that gap, from a network-centric perspective. But this whole data-centric world, maybe it's just because it's little bit more esoteric, but we don't seem to be making that connection.

**Dr. Larry Ponemon:** I think your observation is correct and our research supports what you said about we may be over the hump or may be at the top of the hump for the network-centric, but on the data-centric, there is a ways to travel. I basically think you addressed another issue and that's a cultural issue in organizations. What is the level of responsibility for the developers? I mean developers are under a lot of pressure to get the job done.

And the "get 'er done" mentality is basically means in many cases that you're not going to do everything you can from the security perspective to test the heck out of the application to make sure it works according to plan.

In some cases, the developer doesn't even realize that in the life cycle that someone upstream is not necessarily going to be testing for security and that there is an expectation of that the developer will in fact have that responsibility.

So there are some real issues and the point you raised, which is a really important point. It's not about in-house developers, whereas outsource resources would result in a better outcome. I think it's true in both camps.

In fact, it may be more difficult when you're outsourcing and you basically have no way of visibly seeing what's done for security. So it is a big problem that requires attention and resources and management buy-in.

**Brian Contos:** Now, Larry, I know some of your analysis and some of the survey was actually focused on the cloud and how individuals are looking to move to the cloud or using the cloud today. How does that in app security play together? Do they feel that moving to the cloud is actually going to help things or make things worse?

**Dr. Larry Ponemon:** It's not exactly clear from the results of this study. I will say a lot of the respondents, many of the respondents, believe that moving to the cloud may be premature. They're concerned that even if they have the appropriate SLA in place, that it is unclear whether the vendor is going to contribute to the security problem rather than the security solution. We actually see that attitude among many of our respondents.

I think it's like an outsourcing issue on steroids. Now you're even further away from the work that's being done. If you're basically trying to determine whether something is secure or not, it's like finding a needle in a haystack. How do you actually determined as a desk audit, or from a distance, whether or not an application is secure and that you can rely on it.

I think cloud computing creates another wrinkle and by the way, we as an institute are in the process of doing several studies that touch on cloud security and I'll just give you a taste of one of the findings of our most recent study. Is basically that the security posture of cloud computing providers tends to be at a much lower level then on premises computing.

And that actually, is potentially is a warning sign if you're thinking about saving dollars, or maybe it's flexibility or agility and you're going to outsource or you're going to use cloud computing resources. You need to factor in "So what does this mean from a security perspective?" A lot of organizations aren't doing that very well, they're running to the trough.

**Brian Contos:** Absolutely. Somebody once told me "The cloud's great, but when there is an issue, it's not only dealing with the technical issue anymore. Now there's organizational issues of who to contact, there's SLAs, there's various procedures in place, it's not simply walk into the datacenter and reboot, potentially." A lot of times, not only does it have complexity, but it certainly adds a lot of extra time to the instant resolution, which is something I think people should be aware of.

**Dr. Larry Ponemon:** I agree completely, so if you basically care about security, it doesn't mean you don't use clouds but you need to do some work. You need to figure out how you're going to manage, or collectively you and the cloud computing provider will manage that security responsibility and maintain a certain security posture.

**Brian Contos:** That's a great point; it definitely has to be a strong partnership. So Larry, as we wrap things up here, one thing that I'm really interested in hearing is what distinguished the survey takers who were really more successful with apps.

**Dr. Larry Ponemon:** The first finding, in terms of what actually constitutes a success story versus a failure, is that we do have some organizations that self report that believe that

they have this issue nailed. In other words, they're doing a good job. And we actually try to figure out "OK, so is it just Pollyanna, and you say you're doing a good job and there's no reason why you believe that to be true." We actually found using correlation analysis and crosstabs that what were the striving factors to success. One is pretty obvious, it's called resources.

It seems that the organizations that had more success securing web apps were spending twice as much on average. So it does cost more to achieve a higher level of security in this phase. Let me give you an example. For those that believe they were proactive in managing this risk, it was about 25 percent of their total IT security budget.

Which still could be a pretty pitiful amount, it may require more resources but as 25 percent versus 12 percent of organizations who felt they were not proactive. In other words, they had a huge problem. It was unresolved on their hands.

Another finding is that organizations that were doing a good job were much more likely to use web application firewalls of 43 percent versus 21 percent. It fell into that category with a very weak security posture. And SAS based security solutions were viewed very favorably by organizations that had a stronger security posture over web apps.

Finally, we feel that organizations that were proactive in managing web application security were also much more likely to respond to web vulnerabilities in a timely fashion.

We found that that was very effective from a cost perspective because by not having the resources, it means you're slow to fixing the problem or maybe you're not fixing it at all which basically leads to a whole bunch of other costs like downtime or not having enough time or other costs associated with just not having a good overall security program in place.

So in general, I think the organizations that we might want to aspire to have resources and are using leading edge technologies. One of those happens to be web application firewalls, which is good news, of course, for Imperva.

**Brian Contos:** Absolutely. We like to hear that there are organizations out there that are having success and doing the right things and perhaps leading the trail for others to follow. It seems like applications, every time you do some searching on the Internet or read a newspaper, it's not opaque anymore. We know the target. People are going after sensitive data and that's how they get it. We're just really, really far behind overall as a Internet society I should say, but certainly as a country where I think we're woefully unprepared and very vulnerable.

**Dr. Larry Ponemon:** Well, agreed, but the point here is that the organizations that have these vulnerabilities are not just organizations that are handling consumer data but also some governmental organizations. So not just as business companies are under attack, but it also is applicable to governmental organizations.

**Brian Contos:** Larry, once again, thanks for joining us on today's podcast. It's always a pleasure speaking to you.

**Dr. Larry Ponemon:** Brian, it's always a pleasure doing one of these and I look forward to do many more in the future.

**Brian Contos:** For more information on this podcast and Imperva, please visit [imperva.com](http://imperva.com) or send us an email, [blog@imperva.com](mailto:blog@imperva.com).



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