

## Healthcare Data Security within State Government – an Interview with Gary Lilley of HP

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 us today is Gary Lilley. Gary is a senior enterprise solution architect with 19 years of experience in software system design, development, and implementation with extensive experience in government systems, large-scale chain retail, data management, manufacturing and distribution, and translation software, within the computer industry, banking, EDI, and most translators across all hardware platforms.

He also have extensive experience in sizing hardware and enterprise-wide systems. Gary is currently working on a state-wide database activity monitoring security project having to do with healthcare.

Well, welcome to the show, Gary.

**Gary Lilley:** Thanks for having me.

**Brian Contos:** So Gary, before we begin, could you tell us a little bit about what your job responsibilities are and what the particular organization that you're working with actually does?

**Gary Lilley:** I am currently the lead technical architect for the state agency that is responsible for maintaining public health and awareness. My job duties are to design and implement their real-time pandemic flu surveillance system.

**Brian Contos:** Very interesting. Now when you were brought into this particular project to look at database security within this organization, what was the compelling event that said yes, we've really got to focus now on our database security?

**Gary Lilley:** Basically, we are dealing with the emergency department data, which includes PHI, personal health information, which is covered under federal regulations and must be secured according to those regulations.

**Brian Contos:** Clearly, there are other vendors in the space. When you were in the product evaluation phase, what other products were you looking at and what were the drivers behind you deciding on Imperva's database activity monitoring solution, or DAM?

**Gary Lilley:** We evaluated Oracle's database security product, Database Vault it's called, and also Guardium. The main reason we chose Imperva's was the ease of implementation of the product, as well as the thoroughness of its covering all avenues of the security arena, network and database.

**Brian Contos:** Yes, I hear that a lot. People talking about the fact that they can use Imperva SecureSphere's DAM solution to not just do the audit portion within the database, but also look at the database protocols and the underlying OS that the database sits upon. It seems to me that if you're not watching the network side as well as the local host side within the system itself, you're probably missing at least half the picture of what's going on.

**Gary Lilley:** Well, one of the reports we ran first was a report that goes out there, and checks all the basic stuff in the Oracle database such as default user IDs and passwords, and lists all those risks so that you can correct them.

**Brian Contos:** Well, that's got to be a huge time-saver. I know going through any of those things manually without some type of automated reporting can be a real task.

**Gary Lilley:** Well, and usually, that's a DBA function, but someone has to check that to validate that it was all done when you implement a database.

**Brian Contos:** Absolutely. What is the scope of the current project if we were to break it into phases, and we call this phase one? What's the scope of phase one?

**Gary Lilley:** That was to design and implement the solution. We're now into phase two, which is hooking up all the hospitals in the state to our solution in order to get their emergency department data real-time, or as near real-time as we can.

**Brian Contos:** Gary, when we talked earlier, it sounds like the - I don't want to call it scope creep because it sounds like it's been very, very well detailed in terms of the outline. But it sounds like it's actually quite a massive project across the state in terms of all the various departments you're bringing in. I mean, this is a large undertaking. This isn't just securing one or two systems or one or two programs.

**Gary Lilley:** No. Part of our solution is also to bring in lab data, so we have to have all the labs hooked up in phase two, and over-the-counter, so we also will have to subscribe to the national over-the-counter drug service, which gives you over-the-counter drugs that are purchased every day. Because a lot of people will - especially tourists - don't go to the doctor. They'll go to the local drugstore and buy flu medicine, for example.

Also, there are other departments within the Department of State. For example, the Department of Health will just monitor and get alerts. Then they'll notify the Department of Disease Control on any investigations for any pandemic outbreaks.

**Brian Contos:** Wow, so with a project this substantial; usually when we're talking to an organization about a DAM deployment, there's a handful of key departments that they want to leverage. It sounds like for this one, there might be literally dozens, if not hundreds of organizations and departments that weigh in on decisions here. Is that accurate, was that complex?

**Gary Lilley:** It's complex due to the political nature of working within government agencies. And then you have to deal with each agency's regulations and that type of thing. So it gets very complex politically as well as technically. Some of them are real remote, and hooking up all those hospitals and urgent cares can be technically challenging.

**Brian Contos:** I'm assuming, correct me if I'm wrong, but there's probably quite a heterogeneous mix of technology out there. Some proprietary, some legacy, some commercial; you're probably literally seeing all shapes and flavors out there within this deployment.

**Gary Lilley:** Right, up from no technical ability to do that integration to... They do the standard HL7. So you reach the whole gamut. For those who can't do data integration, we have a manual data entry screen as part of our solution for like the real small urgent cares on the other islands.

**Brian Contos:** The more I hear about the complex environment, distributed, multiple organizations, it's almost the poster child for organizations that can get value by leveraging DAM. It's great to hear cases like this. You've had it deployed for a while; you mentioned earlier that you were already on to secondary phases. Thus far, have there been any interesting findings?

**Gary Lilley:** Yes, we found out that one of the applications we were using for the surveillance system leaves sessions open if you don't correctly log out. So that's an issue of performance as well as security. The other findings are the port where Imperva goes out there and checks all of the servers and the network, and gives a report of all the ports that are listening, so that we know which ports are open, and which ones aren't, which is very interesting as well as concerning.

**Brian Contos:** Yes, isn't it interesting how sometimes those two things go together?  
[laughter]

**Gary Lilley:** Yes.

**Brian Contos:** So Gary, just as we sort of wrap things up here, for organizations that are looking into deploying DAM solutions, can you give them any tips or lessons learned; things to look at?

**Gary Lilley:** Well, the first thing I do after getting it installed would be to run all of these different reports that give you the information you require to make your environment secure. To me, one of the most interesting things was the open port/listening port report, because that's how people back-door into servers with all kinds of bad things. So from my standpoint, that would be number one.

And number two would be the database report that gives you all of your vulnerabilities in the database as its set up and configured currently.

To me, those are very important for understanding and having validation that your environment is truly secure, especially if you're dealing with PHI data or sensitive financial data, or any kind of personal data like that.

**Brian Contos:** That absolutely makes a lot of sense. The more and more I'm involved in these larger database activity monitoring projects, the more people say to start with some initial things that you know you want to find, and run some basic reports. From there you can build a baseline, and perhaps even a template, for how you attack other areas within the organization and other issues.

I think it goes back to, if you want to crawl before you walk, and walk before you run, but... Most enterprise security tools and audit tools, if they're well built, will grow with you and

## State Government Healthcare Data Security with Gary Lilley

grow with the multiple phases that you're adding on, and it sounds like Perfect Secure Sphere is doing that for you today.

**Gary Lilley:** Oh yes, I'm very pleased with it. It has more than met my expectations. I'd never have an interface with the product prior to our evaluation here. So I was pleasantly surprised.

**Brian Contos:** Well, that's always great to hear. Gary, I know you're a very busy man, and you've got a lot more work to do out there. But I appreciate you taking a few minutes today and sharing your insights with our listening audience.

**Gary Lilley:** I appreciate the time, sir.

**Brian Contos:** 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).



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