

Data and Database Security - an Interview with Juan Walker – Data Security Advisor with the Educational Media Foundation

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.

Joining me today is Juan Walker with the Educational Media Foundation (EMF). Juan is a database and data security adviser for the information technology team at EMF Broadcasting, which is K-LOVE and Air One Radio Network, with over 600 stations and translators in 46 states.

Juan has over 15 years of experience in database architecture and administration, and extensive knowledge in encryption and data security. Prior to EMF Broadcasting, Juan worked as a database administrator at Microsoft Corporation, and senior data architect at Georgia Pacific Corporation. He has received certification from SANS and ISC2.

Welcome to the show, Juan.

Juan Walker: Good morning, Brian.

Brian Contos: Juan, where was it that we met? Was it Interop Las Vegas or Black Hat?

Juan Walker: It was actually Interop in Las Vegas that we met.

Brian Contos: That's right. So, it's been a little while. And I know when I was down there, you were telling me about some of the interesting things you guys are doing around data security. I think this will make for an interesting podcast for our listeners.

But before we get into that, could you tell me a little bit about your organization, the Educational Media Foundation?

Juan Walker: We're a nonprofit organization that operates K-LOVE, Air One Radio, and also a third radio network. We're based in Rocklin, California. And the largest network, which is K-LOVE, we have about five million listeners per week. Total, we have 300 stations. We also have a large stream for iPhones too.

Brian Contos: Oh, fantastic. Is that becoming a pretty popular solution now, streaming media directly to the iPhone as opposed to maybe more traditional mechanisms?

Juan Walker: Yeah, we're noticing that a lot, especially in the radio industry, you know, with podcast of radio stations and even video. And we want to do just about all of those.

Brian Contos: So, Juan, what is it that you do for the Educational Media Foundation?

Juan Walker: I am the database and data security adviser here. It's actually my job to protect our data and make sure that it's available. We have about four million donors, and it is important to us to keep our donor information secret.

Brian Contos: Very impressive, actually, to hear that. Your organization actually has somebody dedicated to data security and database security. I understand the donors, is that something that Educational Media Foundation has always been focused on, data security? Is it because of regulations? Was it a compelling event? Why does a position like yours exist there?

Juan Walker: I think the main thing is we just want to be responsible to our donors, and we want to make sure we're making the best effort. And you know, we're using good equipment, good technology, good services. We're surrounding ourselves by good companies to protect that information in transit and at rest.

Brian Contos: What are the security issues that are really chiefly a concern to you guys over there? Is it the idea of an insider threat, external attack? I guess there's some level of competition in information being stolen. You mentioned your donors. What are the key things you're really focusing on?

Juan Walker: Well, it is that protection of the donor information. But, as you just said, you do have that insider threat, as well as the more sophisticated attacks that are happening today. So that's really driving us to place layers of security around our data. But the main thing is just to keep the donors' data private. And as you just said, we are bound by PCI, and we do do several other audits, legal and financial. So we are driven by that too.

Brian Contos: Yeah, these days it's hard to bifurcate drivers for regulatory compliance, governance, and security. While they might be budgeted differently, they all seem to overlap each other in quite a few areas. How do you see data security evolving? And I suppose this is a two-pronged question both from sort of an attack vector perspective, and also from a mitigation perspective, sort of from your adversaries and from your own perspective. What are some of the challenges in data security?

Juan Walker: I think for this year and past years we're going to see attacks emanating from the inside will probably rise. And then it's probably going to be a line blur between internal and external. You might have already noticed that contractors might get a job in your company and use different social engineering attacks. So I see that more, that we're going to have to look at the people who we bring in, the people who will actually do the services for us, and anybody that touches our data from the outside.

Brian Contos: That's a really subtle point there that I'd like to dive into a little bit, this whole idea of data is data, and you think of that at the core. And on one side you've got insiders or privileged users or contractors or partners with access, and on the other side you have everybody that doesn't fall into that bucket. But it's unclear today the line between insider and outsider, I think it's really starting to blur, and it's almost losing meaning. Do you feel that way? Do you feel that even in your industry that seems to be the trend, just because there's so much access to so much information from your iPhone or your laptop or whatever the case might be, that it's really difficult to determine who is an insider, who is an outsider? It's not the old days of put stuff here, stick a firewall in front of it, and you're good.

Juan Walker: Right. I mean, even as you just said, your outsiders can become the insiders because you're bringing in contractors and different services. You're trying to leverage services outside of the company while maintaining a lean IT on the inside. So, yeah, it's definitely being blurred. And it's probably easier; more sophisticated attacks too based on that -- software the user's assigned, even more harmless websites. I could create

a website that even seems harmless, and that is actually an external piece, but your users on the inside click on that, and suddenly these people are on the inside.

Brian Contos: So as the security guru there, essentially I guess you have to - and you sound like you already have - but fundamentally change the way that you approach the problem of protecting data. It is no longer outside versus inside, it's data in general, and irrespective of where the attack might be coming from. Like you said, an external attacker might become an intruder. So, data security is really at the core of a lot of these discussions these days.

Juan Walker: Right.

Brian Contos: So, switching gears a little bit, Juan, in regards to Imperva, which products did you purchase from Imperva?

Juan Walker: Well, actually, we did the Database Activity Monitoring (DAM) piece. And I guess I should step back a little bit and say that we have rings of protection, or layers. So the first layer would be the vulnerability assessment, firewall, vulnerability assessment monitoring, and then finally encrypting it. So we started at the data layer, but we also plan to include the web applications also. Right now I have database activity monitoring, but I'm planning to get the web application firewall piece, and continue to add those different rings or layers to our database security and data security.

Brian Contos: There's definitely a lot of symbiotic mutualism between the web application security solutions -- just in general, not even talking about Imperva -- and database security solutions. Having one without the other is valuable, but having the two together really gives you quite a robust solution. Now, I'm interested. When you said vulnerability assessment, that means a lot of things to a lot of people. Are you talking about application and/or database-specific assessments, or more of the traditional network layer, or are you talking about both?

Juan Walker: OK. We do all of those. We do application vulnerability assessment, database, and network. So that's part of our layer. Now, your tool also has a vulnerability assessment, but I also have an outside company that does the same. So I'm getting it from a database perspective, with those database-specific vulnerability tests. And then I have another company that's doing it from the outside, from the outside into our company, and inside-out. So I think I'm covered in vulnerability assessment and monitoring.

Brian Contos: And you mentioned that your drivers were protecting your data for donors and various regulations, like PCI. So you have both a security, just general judiciousness, as well as a sort of regulatory plan. What's changed about your approach? Or maybe nothing's changed. But what's changed about your approach since adding the database activity monitoring, the DAM solution, in place? Has it given you visibility, or has it provided any early wins since you've installed it?

Juan Walker: Actually, it has. As you know, with databases in large environments, you have pockets of data, or islands of data, throughout the company. From the first time we turned on a discovery, I found instances and places that we needed to look at. And that was one of the biggest wins. We're also getting ready to go through an audit, and I've found the reports invaluable for that.

Brian Contos: Yeah. It's always amazing to me when somebody does discovery, and sometimes they find even databases that they weren't aware about, but certainly data within those databases, certain tables and things that contain information that they weren't

aware existed there that has to do with... Sometimes they're rogue databases, but sometimes they're replicated or they're backed up. They're used for testing. They might contain some information when they were doing that. The developers might have backed up all the sensitive data as well, or replicated it. So that's really interesting.

So you've got the database activity monitoring solution, and it sounds like you've got multiple layers of security, I'm sure, at the network layer as well as the data layer. And you mentioned that you are looking to add in the web application firewalls as well. What's sort of the driver behind that? Is it to have a more holistic perspective on your data-security environment, or were there some very specific reasons why you wanted to add WAP to the solution?

Juan Walker: Yeah. From a holistic approach, and I guess where you place the web server, it could actually become an endpoint. So with that, the web application is the gateway to that protected zone, that confidential data. So we want visibility in all of that, into the web, from the external-facing all the way into our internal network.

Brian Contos: Fantastic. That's a great approach. So, Juan, obviously you're a large organization. You're dedicated to this task of data security, and you evaluated probably a number of various products and competitors. What were some of the things that you were looking at, and ultimately, why was it that Imperva was chosen as the right solution for you?

Juan Walker: Probably the ease of introducing a new piece of equipment into the environment. And I looked at several solutions, like you said, and the Imperva solution seemed to have the lowest overhead, and the flexibility in introducing it into our environment. You already know this. You've got the inline solution, and you can do standard report or you could do agents, and we might have a situation where we could use all of those. And that made it more attractive to us.

Brian Contos: Definitely, flexibility and the ease of use is a chief concern for a number of customers. Are there any features in the product that you were just like, "Wow, this is great. This is the feature, or this is the report, or this is the capability that really, really addresses our needs"?

Juan Walker: I really like the reporting. I really said wow when I saw the monitoring and the discovery. The discovery was the piece that I was really impressed by, as well as just how well-built the site is in general, and how easy it was integrated into our environment. You know that the other solutions that I tested just didn't seem as robust. Yours is the total solution.

Brian Contos: I think you said it best. You wanted to scale it up and ultimately add web application as well.

Juan Walker: Right.

Brian Contos: As well as having robust data for the complete data store end. Unless I'm mistaken, I don't believe there's another game in town that does it so cohesively.

Juan Walker: No, I would agree with that.

Brian Contos: Great. Well, Juan, we have time for just some closing comments. Is there anything that you'd like to say to the audience just about data security or Imperva in general.

Juan Walker – EMF

Juan Walker: Yeah, the Imperva database activity monitoring solution is great. Because we were trying to achieve depth in defense, we wanted to add more layers at the perimeter to maintain integrity, and we also want to make sure that our systems are available. And yours is key to us discovering whether that confidential data might exist, whether it's at one of our external sites or right here in Rocklin.

Brian Contos: Fantastic. Well, Juan, thanks so much for joining us on today's podcast.

Juan Walker: Thank you for having me.

Brian Contos: For more information on this podcast, and Imperva, please visit imperva.com. Or send us an email: blog@imperva.com. **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.



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