

Data Security – an Interview with John Pironti – President of IP Architects and Interop Chairperson

Listen to the 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, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Brian Contos: Joining me today is John Pironti. John is the president of IP Architects. He has designed and implemented enterprise wide electronic business solutions, information security programs, business resiliency capabilities, and threat and vulnerability solutions for key customers in a range of industries, including financial services, energy, government, aerospace, media and entertainment, and information technology on a global scale.

In addition to having many industry and vendor certifications, John is also a published author and writer, highly quoted and often interviewed by global media, and a frequent speaker on electronic business and security topics at domestic and international industry conferences. John is also a program chair for Interop.

Brian Contos: Welcome John.

John Pironti: Hi Brian, how are you today?

Brian Contos: I'm doing great, thanks for joining us. Before we get started I'd like to talk to you about some of the things you've been working on. You had mentioned a little bit about information security and information risk management earlier. Can you dig into that a little bit?

John Pironti: Yeah, sure. I think what I can say I've found in my work and doing this work on a global scale amongst many industries, in that the last 10 years we've really started to appreciate the fact that security's an important concept within the enterprise.

What we've done with security though is that we've typically taken it down the path of fear, uncertainty, and doubt, saying that certain technologies will present certain hackers or certain activities from occurring. We know this because we have good technology, we have good tools and capabilities, and we have good nerds to understand what's going on with our technical infrastructure.

What we don't have is business alignment. When you think about the concept of risk management, that really drives business alignment. In fact, sociologists will tell you that the word security has a negative connotation to people. When people hear security, they think you're going to prevent them from being successful. They're going to stop you from doing something that you want to do.

Security professionals have often asked to get in front of the business or to get ahead of the problem or be brought in early. But they always are bringing together tools and capabilities

that are just doing that, preventing people from being successful because that's all they know. That's what they have in their toolbox.

What I've been driving towards, and what I've been helping organizations develop and build is governance models and processes and capabilities that change the direction and change the tone of the conversation we have. We move from information security to information risk management, which encompasses a whole bunch of the elements in information security, but adds things like business alignment, strategy and marketing alignment, public relations activities, business continuance and business resiliency.

Lots of other elements, physical security that with other systems we weren't putting into the security conversation and adding security as part of a module as well which then gives us an overall perspective to bring to the business an understanding of, here's what we think that we're prone to be dealing with.

Here's what the threat and vulnerability analysis has said to us that we need to worry about. Now you need to make the decision of what we want to do. What should we approach, what should we do? What is our acceptable level of risk? It can no longer be a security person saying, "You have to do this, or else."

Brian Contos: I think that really resonates with a lot of organizations today. Because if you think of security, for certainly the past few years, it's really moved away from this pure technical discussion to one that's being taken into staff meetings and board meetings. In these types of groups cyber security is just one of many forms of risk. Doing business in a different country is risk, doing business on the Internet introduces risk, purchasing another company has risk. For them, it's all about risk management.

John Pironti: Absolutely. That's what the board level conversation wants to have. Most CISOs today get fifteen minutes of fame with the board a year because they're forced to because of compliance requirements and such. Essentially they're going in and telling people about hacking attempts and things that happen in the world, but the board moves on.

Because the board realizes that they have to be able to do business given all the bad things that can happen in the world, all the challenges. If security stops them from doing their business then there is nothing to secure. There's no business to do. So we need to establish acceptable rates of security and risk for information just like we do for other parts of the business and then align our control frameworks and our activities to those risk profiles.

Brian Contos: From my perspective, when you think about business and what the valuable piece is really, it was easy 10 years ago to think about things in terms of firewalls and IDSeS, and not a lot of talk was around data security. When you hear the term "data security," what's that mean to you?

John Pironti: Well, data security still means, to a lot of people, technology. It still means what is the tool, what is the thing I'm going to surround the data. What am I going to put around it as a wrapper?

In my mind, I think data security is really information security. And it's following data, understanding where it lives, where it is, what's going on, and also understanding that not all data's created equal.

A lot of times, we build these networking tools and application security tools. We build these things that basically say all data's going to be treated the same way. But in reality, all data

doesn't need to be treated in the same way. Different data has different threat and risk profiles associated with it.

And thus, when I think about data security, I think about what is the data, what is the business process that is associated with that data, what is the value of the business process to the enterprise, and then what is the acceptable risk level based on that business process? Then we drive down to understand the control frameworks that we apply to that data, which then becomes data security.

So, after we identify the risk profiles and the things that we're going to align to in our acceptable levels of issues and of attacks and challenges, we then can bring in the security guys and say, "All right, build me control frameworks that align to this risk profile for this data type."

Brian Contos: Well, let's expand a little bit on that. So we're talking about the control frameworks, and we're talking about the areas where the data is processed and the data is stored, which is typically applications, maybe web applications, maybe SAP applications on the back end and what have you, as well as the critical databases. How do you see security really starting to get more embedded with these types of systems that have historically been a completely disparate organization or disparate group within a company?

John Pironti: Well, I think it's a great question. And my view and the program that I've built for many organizations, small and large, all over the world, is really more of a consult to the group.

My belief is that information security within an enterprise is a consulting organization, not an operations-driven organization. There are operational elements that can be part of the organization, and that typically comes into play during incident response and business-resiliency activities, when the standard operational staff isn't enough to solve the problem, once it gets beyond that first tier of capability.

So, when I start thinking about this kind of overlay structure and I look at how things are changing and embedding themselves, I think we're getting closer and closer to the information. We understood, years ago, that perimeter security wasn't enough but was still important. Now we're starting to appreciate the fact that if we could write better source code, that would help us from having a lot of the exposures that we have.

But in reality, even the best-written source code, applications that are written exactly the way they're supposed to be written can still have challenges. We still can have business processes that were designed improperly or activities that were designed improperly that, given the right code and all the right tools, still can be compromised.

Think of a web environment in this way. We still let traffic come down port 80. If we let somebody do a database call, some SQL command, somebody can pull data if they're able to harvest somebody's ID. And if that ID's valid and accurate and authenticated, then the system's doing exactly what it's supposed to do and you still have the compromised situation.

So I think we're raising up the bar slightly, as we're starting to clean up some of the things that we realized were getting harder and harder. I think a lot of people were very fearful of application security for a long time because they realized the idea of going through and really going into the applications themselves and finding all the source code and doing code-walks and things like that is extremely time-consuming, is extremely expensive, and it doesn't really always find everything we need to find.

But in reality, this is kind of what we're doing now, right? A lot of people are taking the time to look at their code and say, "Let me work on that part of the puzzle, as well as my perimeter, as well as my database security and authentication mechanisms. Let me start wrapping more layers to try and give myself a fighting chance, from the noise. Not from the very experienced, not from the very smart and very capable adversary, but from the adversaries that will go online and download some generic tools and try and run them against my environment."

Brian Contos: If you look at the dichotomy between, let's say, a network-vulnerability scanner and an application-vulnerability scanner and compare the output, well, most security professionals today, they really get the network-security vulnerability output information. They get that.

But when you start looking at application vulnerabilities and database vulnerabilities, sometimes this is a completely new thing to them. Do we think we're going to start seeing a different breed of security professionals, ones that are tied more closely with the application and database side? Or do you think these are really going to remain two groups? You've kind of got your network security guys, you got your application database security guys, and they're not necessarily the same team.

John Pironti: I think that it's going to be a combination team. I think they're two different skill sets and two different approaches. A lot of guys are really good at networking and network environments.

They understand hardware in that area, really never got into doing coding. They didn't go through the ranks of computer science and understanding assembly and C and Java and all the languages that we use today. And they didn't need to and probably still don't need to. Their direction and their mentality and their interest doesn't bring them to that area.

I think that the application security environment's going to come through specialties coming out of the teams who are actual coders. It's going to be an area of advancement, a promotion area where people are going to come through the development groups and start becoming better at teaching programming and helping people understand how to look at code better, and look for challenges, and look for problems.

I think also we're getting to some of the common problems already through some of the automated scanners. Although, they're not that effective based on the current stats we have on them. They're not finding nearly enough of the problems that are still sitting out there. There's just way too much code out there right now.

Brian Contos: Do you think that stronger regulations are the future? I'm seeing a lot of predictive analysis coming out now for 2009. You're out there in the field, and you're talking to people. Is this what you're seeing?

John Pironti: Absolutely. Not just in the United States, but abroad. We're seeing a broad stroke increase in regulation. Everybody's trying to find a way to force people to meet base line requirements. Why? Because they've now realized that data has a value and that information has value. That value was always there, and the risks were always there, but we didn't ever have it collected in such a way and accessible from such long distances before in the way that it's become over the Internet and over the web.

Across the world we're starting to understand that we do need to install certain regulations and capabilities to create base line capabilities. I think the greatest example I know of this -

and I've talked to peers who have thought through the same thing - is the idea of the seatbelt in the car.

For many, many years we didn't have seat belts in cars. Then all of a sudden they started appearing. The first seat belts we had weren't really that good. The first seat belts were only lap belts. Those lap belts ended up causing a lot of internal injuries and a lot of more deaths than they did positive in some cases. Until we finally got to the shoulder belt, and the airbags, and we started adding more and more systems as we made matured the environment.

I think that's what we're going through right now in the security world. We're establishing baselines. We realize that there are certain things that we need to account for, but you also have a lot of things that we are putting in place that may be doing more harm than good, especially on the technological front.

When you start looking at things like forced encryption of data everywhere and anywhere. I think that that's causing tremendous problems for people right now. There's the idea that encryption is going to solve the problems of the world really doesn't really help. It actually hurts in a lot of cases. It reduces the ability to look at data, to investigate traffic patterns, to understand behaviors.

My view typically on this is if I'm in a physically secured environment where the data is in a data center or a drive array, and I've got this locked down with other measures, then what's the cryptography going to do to help me? It's not really going to do anything but cause me a lot of grief and pain for key management and staff and move costs around and things like this. But it sounds good. The regulators have heard about this and they like this concept. They've gotten on the bandwagon since smart people told them it was a good idea.

Now we're seeing regulations that are driving these concepts, and we're getting that checkbox approach. The checkbox approach is my biggest fear we have on the worldwide scale right now. I call it security by compliance. That's if I just do what is expected of me minimally by the regulator or by the external party, then I'm doing what could be asked of me. I'm not doing a risk based approach, I'm doing what somebody else thinks is right for my business. I can tell you that no one else can tell you what's right for your business except you.

Brian Contos: You know what that reminds me of? Encryption, today, sort of makes me think of network based firewalls 10, 15 years ago when people said, "Are you secure?" "Yeah, of course we're secure we've got a firewall." "Well are you secure today?" "Oh yeah, we're using encryption." I think it almost gives them a false sense of security.

Then they're not taking the pragmatic measures to address other areas and controls within their organization because they think that they have this catch all behind them. I think - to your point - I think it could possibly make things worse. Like you said, you're doing the least common denominator, security by compliance. We've got encryption, we've got network firewalls, let's move on - and that they're not paying close attention anymore.

John Pironti: Conversation at the board level is what is being asked of me, so I'm able to put a dollar value about what I have to do. A lot of people are saying, "As long as I just do that thing, like the PCI or GLBA or the EU data, privacy data security requirements. As long as I can say I'm meeting those, then I'm doing everything I need to do for security. I can put a dollar value around it. My risk is not about protecting data, it's keeping myself out of the courts and out of the court of public opinion. To say, look I did everything that was asked of me."

That's wrong. That's where other people tell you what the best practice is. And I'm here to tell you, I don't believe in the constant of best practices any more at the industry level. I believe there are industry leading practices. Things that we do in lots of places that make sense at certain time. Security, as you know, is a moving target and things change. I think that leading practices are things that we know are working right now. Only organizations can decide what the best practices are for themselves.

Best practice is a term that was invented by the legal community to try and trap people in court environments. Because what you may believe is a best practice may be completely different than what I believe is a best practice. It's almost like the unstoppable force and the immovable object. What happens when they come together? Who do you believe?

Brian Contos: Something that I think is going to start grabbing a lot of headlines - it's certainly been all over the press for the past couple of days - is that President Obama has actually declared the country's computer infrastructure as a national asset. He's actually going to have a cyber advisor reporting directly to him. You and I have worked with government agencies for quite some time. Do you think this is the wakeup call? Is this the point where we're going to start seeing better security around national security and critical infrastructure?

John Pironti: You know, Brian, I'd really like to believe it is, but I'm not sure we're going to get there with this one. We tried this with homeland security. We created the cyber tsars, and three cyber tsars left very quickly because they were astonished at how little budget they were given or how little attention they were given. Politics by nature have different direction and different requirements and can be moved in different ways through lobbying activities.

I'm appreciative of the Obama group and the Obama presidency that's going to put a cyber tsar in place. I think that the acknowledgement that information technology is important enough to have a direct understanding of its impact on our economic and critical infrastructure for life safety and such for the nation is important. I like the fact that it's been recognized, but I'm not sure that that's going to get the job done. Because a lot of what we're doing with the problems and the challenges we're having with our critical infrastructure is more about getting the right people to understand where money needs to be spent.

Right now people want to spend money where they're going to see immediate impact in things that they can touch and feel and have in front of them which is why physical security always gets so much money. Information security and data environments, that's a hard thing to substantiate. Sure we've had a lot of data breaches, sure we've had a lot of accounts breached and that's been painful, but we also have a desensitization that's happened at this point. People are starting to get desensitized to these things and not front page news anymore. They're fourth page news.

We need major incidents unfortunately to prove to us that we need to do more and more and more in this area. I think that's what the government responds to, is when we have an incident. Then they will put controls in place for at least a short window of time to say you need to do this better. You need to have this in place. We've seen that already with the data disclosure laws. We saw that with many cases. We've seen this with other situations.

I think that the next big trigger's going to be if we have a disclosure around healthcare records. The thing about healthcare records is that they can't change. They stay with you throughout your life. So if your healthcare records are disclosed in some way, in a public

fashion because of some loss at the government level, it's going to look really bad. That's not something where I can just change an account number and everything goes to being OK. That's something that somebody's going to have to live with the rest of their life, that that information's been made public.

That's what I think it's going to take for the government really to step up and say, not only am I going to create a cyber tsar, but I'm going to fund that cyber tsar, I'm going to start bringing in talent from the commercial side to help us as well. It's not going to be that not invented her syndrome that typically comes out of government agencies. They're going to start learning from what we're doing at a risk based approach in the public and the commercial side to say, "What do I really need to do?" Versus what do just do to get along.

Brian Contos: All great points. Well John, as always, this was an absolute pleasure talking with you.

John Pironti: Thank you very much Brian. I appreciate the time.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at 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