

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.

Luiz Eduardo: Welcome to our podcast. My name is Luiz Eduardo dos Santos, Senior Security Engineer for Latin America. Today, I am taking the place of Brian Contos, Chief Security Strategist of Imperva. With us today, in our first non-English podcast, we have Rafael Koike from Telsinc.

Telsinc has been active in the Brazilian IT market since 1994, offering advanced solutions and professional services. They are recognized as a company that is agile, experienced and innovative in the utilization and operation of information technology.

Rafael has been with Telsinc since 2006 to help develop and grow the IT Security business within Telsinc, offering complete solutions from the perimeter to the end point. He has more than ten years of experience in networking and security field having previously worked at Siemens. Rafael holds CISSP and CISM certifications in governance and administration. In addition, he is technically certified CCSE Checkpoint and CCNP Cisco. Due to his contributions, Telsinc's IT Security division has grown an average of 33% annually with estimated revenue of over R\$11m in 2010 in hardware sales alone.

Hello Koike, how are you?

Rafael Koike: Hey Luiz, good, thanks.

Luiz Eduardo: Rafael, are you ready for an important discussion about the application and data base security market in Brazil?

Rafael Koike: Of course, absolutely. Let's go.

Luiz Eduardo: Great. This is important because it is the first Imperva podcast that will not be in English. We will do a great job.

Rafael Koike: I am honored.

Luiz Eduardo: Let's begin. Explain to me a little about Telsinc's activity in the IT security market in Brazil.

Rafael Koike: Well, Telsinc started in the IT market principally as a solutions based seller of networking infrastructure. One of our largest partners is Cisco and we became specialists in the area of switching and routing. As time went on and we grew, we expanded our product and service offerings into IT security. If you look at the last five years, Telsinc has increased partnerships with security companies to complement our solutions portfolio. Telsinc is growing fast in the security market, offering not only products but services as well.

Luiz Eduardo: Speaking of solutions for the market, in your general opinion what is your view about the market for data security in Brazil today?

Rafael Koike: Well, the demand grows more each year in Brazil. I see that initially companies, our clients, began looking for DLP (data loss prevention) tools, to control the escape of information from user workstations. The great challenge today in Brazil has to do with the maturity of IT security in companies. Many companies still do not have well defined security policies; one can't accurately classify this information correctly. In other words, I do not know what is important for my company. If I create some information, how can I define if it is confidential or if it is public information? This is the first step, I think, that Brazilian companies are facing. With that challenge, defining what is confidential and what is public, you can then more easily implement a Data Loss Prevention tool. As well, many Brazilian companies need to meet compliance, such as Sarbanes-Oxley and PCI. Now, Brazil is catching the PCI wave. Many companies that deal with credit cards have to meet this mandate. This forces these companies to look for creation of security policies, develop their security department, in order to create classification rules for information. Once the labeling of information is created, with that, these companies begin to look for tools that will assist in classifying information and controlling access to it. Now, the moment is arriving when companies have a defined security structure and seek tools to help control, audit and block access to specific information. I believe that who is pushing for this primarily is the finance market. With that, they will take the whole retail market and all the companies that deal with credit cards, then in time other companies and other markets will seek this same level of maturity.

Luiz Eduardo: Maturity, that is what I wanted to discuss, it seems as the IT security market in Brazil has really reached a maturation point.

Rafael Koike: Right, also because, I think the market has been waiting for the availability of tools that can help in this process. So, the market began delivering tools to help in the DLP process, helping in the process of securing data, and with that, you promote clients and companies to use these tools. To get to this point to use these tools, they must be mature in their processes and this generates a cycle. I think they are evolving together.

Luiz Eduardo: Tell me something, in your opinion, why is securing applications and databases important for companies and government entities in Brazil? Not mentioning last week's blackout.

Rafael Koike: Well, I was going to mention that case.

Luiz Eduardo: Mention lightly then.

Rafael Koike: Why?

Luiz Eduardo: Sure, speak about it.

Rafael Koike: There is an evolution of hacker attacks and security solutions implemented by companies and government entities. Hackers, or better yet, crackers. I want to use the correct jargon. They have come from attacks directed at network infrastructure and are now breaching applications and databases to do their invasions. Another very important thing is that the objectives of the primordial hackers were to define a status. In other words, do a page defacement was more important than making money. The cracker wanted notoriety. Today, the attacks are against companies, directed at financial ends. In other words, he would rather invade an application of a system, collect information that later I can receive

money with it, I can sell it to someone, I can use it to buy some product, have some status. I would rather enter secretly an application and stay hidden, stay behind the application.

Luiz Eduardo: And then use that later, take advantage of that exploit. Before, it was fun and profit. Today it is profit and not just fun.

Rafael Koike: Exactly. Then, what happens, the hackers won't target my network infrastructure to try and take it down. They will attack my applications and stay hidden behind it. So, database security and application security, I think is the focus today for protection against the threat that hackers and crackers try against your network. These people are migrating from the firewall, IPS environment, which is consolidated, and offers greater protection. With regards to applications and databases today, companies are still looking at it from the other side of the prism. In other words, I have a web application and I don't natively think of protecting it, I have a database and don't think automatically of protecting it. Many times, the web application has a username and password for the database, saved or hardcoded programmed in its source code. In other words, I have a variable username and password, hardcoded in the .php, or in the.asp. There is no reasonable security for that, I have one username and password to access my database and this is a point of failure. In the future I am sure this will evolve.

Luiz Eduardo: Of course. In the same way that attacks came out at the network layer and are moving up in the OSI, today they are at the application layer. Who knows where they are? This doesn't even address internal fraud which you may address later. You had spoken about compliance earlier, let me ask you, in the Brazilian market, what is the role of compliance such as PCI, SOX, etc.

Rafael Koike: I think it is becoming more important, because many Brazilian companies have operations outside of the country. In the United States, for example, so, being in compliance with Sarbanes Oxley, is almost obligatory for a company that wants to do business in America. In this whole global market, it is critical for a company that wishes to grow, increase its sales volume, be in compliance. In addition, many companies that don't sell in other countries want to be in compliance to demonstrate the seriousness of the company, to demonstrate what it really sells, its audited numbers. So, it becomes a differentiator for national companies, even if it will not sell abroad. Many times, they will be in compliance with international mandates.

Luiz Eduardo: Exactly. This complements well what you had previously mentioned. Let's say, the evolution of the market, levels of solutions, etc. Today, it is more than simple protection, the age of just putting a firewall, configuring it correctly, be sure the networks is safe...we've already gone past that phase. Today, we are in a phase, as security professionals, we need to prove, for internal policies or compliance that the firewall is really protecting all it should be.

Rafael Koike: I think the market has changed completely from the objectives of IT from ten years ago to what it is today. Ten years ago, you had the necessity to connect to the Internet to view a webpage, of some site, to surf recreationally. Today, being connected to the Internet means making money. In other words, you improve your income being present on the Internet, when you optimize your online payment system. Sending your banking transactions via the Internet or paying your employees. So, today the job description of the Internet, or IT, is much greater and has a financial impact that did not exist 10 or five years ago. Back then, if your website was not available, it did not have the tremendous impact of today. All our information is digitalized, it is in databases, web applications, and there is web access. Today people expect a quicker transaction time than

five or 10 years ago. So, it is fundamental today to offer that security, not only because your site will be up and running. But also because today's application environment you can lose money. It is absolutely fundamental to have security today. Complement this with the risk of losing money and compliance. The area of information security today can be justified by these requirements, something that 10 years ago, investment in IT security, was a cost for the company, in other words, not justifiable, you could not justify high investment. Today, it is almost automatically justifiable, simply due to compliance or the financial risk, which you can measure with risk analysis. Today, what is IT security and securing your applications can be justified.

Luiz Eduardo: The famous Return on Investment (RoI), discussed in all parts of the world.

Rafael Koike: That's right. Because before you could not incorporate the area of security within RoI but as a cost. Today, it is understood, you can demonstrate this as an "abc" to your clients and to your executives.

Luiz Eduardo: Correct. Now, a more difficult question. Two things about the world of security, what keeps you up at night, except for the blackout, that can help people sleep at night.

Rafael Koike: The question about being in compliance is something that always leaves people thinking. Also, the question about SAAS and Cloud Computing, this also keeps you up at night, because it is a paradigm shift that we are beginning to experience. Cloud Computing, taking information out of your environment and sending it to the cloud. This is a huge discussion between withing our colleagues of information security. How can I guarantee that information will continue with integrity and be confidential? In terms of government, how can a government send its information that today is in its environment, in its possession, to an external environment and guarantee it will not fall into the wrong hands, other countries, political enemies. That is a great challenge today.

Luiz Eduardo: In technology terms, maybe no one has thought about this. Who knows if your data is sleeping at your arch enemy's side.

Rafael Koike: Right, I keep thinking, for example the United States, that has lots of pressure for national security. Could it be that at some point the government will adopt Cloud Computing? How will that happen? How do we guarantee that will function? I believe that is a great challenge today, the Cloud, for government and companies. Also, some companies also are questioning whether they should go to the cloud and how that will happen. This is a great challenge.

Luiz Eduardo: So, since we are on the Imperva Podcast, let's talk about Imperva. What are your opinions on DAS, WAF, DAM and DBFW, speak a little about each of these solutions and how they together bring benefits to the market.

Rafael Koike: Imperva is a company dedicated to application security and databases. That is a great differentiator in relation to other companies. Even at Telsinc, we did not have a partner that could offer these solutions to address the market demands. So, as we are coming out of a mature market, like infrastructure security, and starting to look at database security. Imperva has a critical role in this market. With regards to DAS, it is a tool that will greatly help augment database security, because it will analyze my network environment, discover databases that I may not be monitoring, that I have not yet analyzed. Then, it will monitor those databases and detect if I have that same information in other databases, if I have confidential information in those databases. It will help me categorize, help me know where my sensitive data is in my databases. With WAF, together

with Dam and DBFW, they form a unique solution that I do not find anywhere else in the market. It can detect the IP address of the station somewhere on the Internet, the user from that station that is logging into my application, with wich database he is connecting, what query he is doing. That complete vision will generate excellent audit data, that today I cannot generate. In other words, with out this solution, my forensics analysis for whichever type of incident is totally manual and with faults. If I can have a tool that helps me automate this process, looking 24 hours per day who is accessing my application or who is accessing my database, I feel it is an incomparable differentiator in the market. Imperva is clearly in the front of its competitors, together with Telsinc, to offer this for its clients. We are in the beginning of the wave, the beginning of the market for application and database security.

Luiz Eduardo: Great. And to finalize, what is your forecast for the Brazilian security market, in the near and not so near future.

Rafael Koike: I understand that the Brazilian market is becoming globalized and is much more in synch with what is happening in the American market. So, normally, the market tendencies dictate that at first something is adopted in the USA and generally it would take five yars to begin maturing in the Brazilian market. This time, this delay that exists between the American and Brazilian market, will continue shrinking over the next years. In other words, I understand that in the short to medium term, the tendencies of what is happening in the American market will also occur in Brazil in more rapid fashion. This is because, I think looking that the world bets on Brazil, that Brazil is the future, it is an emerging market with much future. I think it makes a lot of sense what I am saying, that Brazil will be closer to America and other developed nations.

Luiz Eduardo: That's it, Koike. I appreciate your presence in the Imperva podcast. I am not sure if you have some final words here.

Rafael Koike: Well, I appreciate very much the chance of being the first Brazilian that is doing this first podcast in Portuguese. I want to say to the listeners that will hear this podcast in Brazil and the world, that the Brazilian market has much to contribute to the evolution of security tools. Undoubtedly, I believe Telsinc will be a tremendous partner for those clients that are looking for security tools for databases and web applications. So, that's all, that is my message of appreciation to Imperva and my message to those listening to this podcast that we are very optimistic about this relationship with Imperva. That's it.

Luiz Eduardo: Thank you very much Rafael.

Rafael Koike: Thank you Luiz.

Luiz Eduardo: If you would like to know more about topics discussed in this podcast or about Imperva, please visit our web site <http://www.imperva.com>, or our blog <http://blog.imperva.com>, and also you can follow us on twitter, twitter.com/imperva, or you can even email us blog@imperva.com



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