

Data Security in APAC With Terry Ray

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 Terry Ray, senior director for Americas and Asia-Pacific technical services for Imperva. At Imperva, Terry manages teams of security engineers and has designed and deployed data security solutions and performed data penetration testing for a wide range of healthcare, financial services, government, and e-commerce organizations.

Terry has been a frequent speaker for ISSA, OWASP, ISACA, IANS, and many others. Prior to joining Imperva, Terry worked in a variety of technical roles at Check Point Software Technology, including security engineering and partner and end-user technical instruction. Terry has lectured on general network-security topics and taught professional security-related product certifications in over 35 countries worldwide.

Welcome to the show, Terry.

Terry Ray: Thank you.

Brian Contos: So, Terry, before we get going, we have, of course, gone through your bio already, but could you give the audience a little bit more detail on what exactly it is you do for Imperva?

Terry Ray: Sure. At Imperva, I manage and direct the operations for technical sales engineering in the field, typically for pre-sales engineering. I do that for Americas as well as Asia-Pacific-Japan. And really what it means and what it comes down to is I, of course, work with different field managers to work through the specific deals that we have going for any particular quarter. But also I go for example, specifically to APJ. I travel to APJ and work with the customers, oftentimes in competitive deals, but also go and evangelize technology, evangelize new features, as well as talk about corollary technologies to our own.

Recently I was in Japan speaking about cloud security and virtualization, which I think is a hot topic worldwide, but for them it was something that they wanted to talk about. And I have another, similar presentation occurring in Japan, again with a different partner, coming up soon.

Brian Contos: How often do you go to APAC-Japan?

Terry Ray: I typically go to APJ about eight to 10 times a year. That's spread across China, Japan, Thailand, Singapore, India, Australia, et cetera. So it is a diverse mix of cultures and regions, et cetera. But across the board, it's about eight to 10 times a year.

Brian Contos: OK. Well, that's quite a bit. What's really their general consensus, based on your interactions, on data security? And perhaps, as an additional question, is it different based on region? Do the folks in Thailand view it different than the Chinese or the Japanese? I just want to get a sense of, how important is data security over there?

Data Security in APAC

Terry Ray: I feel that data security is important across the world, worldwide. Even in APJ, where you've got a little bit less restriction, a little bit less governance than we see in Europe, Middle East, and Americas, you still see a desire to have data security. The problem that we run into is, while there's a desire from an IT level for data security, there's not always a budget or a pressing need for it, so the budget goes elsewhere. So there's not always the driver that we have.

PCI is certainly relevant there, but not quite as important to them as it is, maybe, in other regions. And they don't have things like Sarbanes-Oxley in all the regions, especially with the teeth that we have here in the United States.

So the pressures that you see in Americas, and even in Europe, you don't see as frequently in APJ. So while data security is critically important to them, they don't always have the incentive or the drivers to get the money that's going to be able to get them the security that they ultimately want and need.

Let me add to your second question, which was by region. Interestingly, each region's a little bit different, and I mentioned SOX as an example. In Japan, we have J-SOX. In Korea, you have something that's coming around called K-SOX. It's similar to what we have in the States, but, as I said earlier, it doesn't really have the same teeth. And as you get into, say, China, you start to lose a lot of the compliance that you would have elsewhere, with the exception of PCI.

Brian Contos: So it sounds like a lot of the data security drivers are actually just coming out of security budgets more so than regulatory compliance budgets at this point, and that's perhaps why the adoption seems to be a little bit slower.

Terry Ray: Right. The best case scenario is that you have IT directors, IT managers, and IT professionals that have the say about their budget, and they can build their budget based on best-case practices. And that's what we see frequently in the territory is it's best case to do this because different analysts say so. So they're taking the lead of other countries and other territories, in many cases. I know I've gone and spoken to banks, for example, in some of the Asian territories. And what they want to know is they want to know, "What are banks doing in America? What are banks doing in Europe?" because they want to do the same thing, even though they don't have the same mandates that those banks may have.

Brian Contos: So what seems to be hotter on the data side? Is it more application security, with a focus on web application firewalls, or is it database security, with a greater focus on database firewalling or database activity monitoring? And the reason I ask that question is, I travel quite a bit in Latin America, and I notice, just between two of the biggest markets -- we'll use Mexico and Brazil as an example -- in Mexico, for example, the database security is extremely hot, where Brazil, it's all about web-application security, and on the vice-versa, it's very much a tertiary topic. Are you seeing one more popular than the other in Asia, or there's certain regions where one is more popular than the other?

Terry Ray: Yeah. So, in Asia right now, certainly application firewalls are, I'll say, marginally more important, or more popular, than the database products. Now, as you said, regionally, that's a little bit different, right? So if I talked about Thailand, application security is the predominant leader in terms of the data security, if you will. If you look at Japan, it's somewhat the same thing. If you move into China, you move into Australia, database security is about 50/50 with what we're doing on the web application firewall side.

Data Security in APAC

So I believe that a lot of that comes down to where you have the mandates, to some degree, but also where you have a little bit more maturity and a little bit more knowledge of what organizations are doing outside.

And as I mentioned earlier, a lot of these countries and a lot of the organizations in these countries look to what other people in other countries are doing. And web application security seems to be a little bit more mature of a technology and of a market than what database security is. It's my personal opinion, but I believe that that's one of the major factors in terms of why we see it being a little bit ahead of what we see on the database side.

Brian Contos: So, Terry, you have an interesting exposure. You work with a lot of large government organizations and enterprises, all over the world, and then you also get a lot of exposure, of course, in Asia. In the news, it's hard to go a week without seeing something about some type of intellectual property theft and someone suing a Chinese organization or the Chinese government. A lot of this IP theft and this hacking that's going on, I guess predominantly focused from organizations or individuals in mainland China.

Do you feel these things are government-sponsored, based on your opinion and your conversations you've had? Or is this just random, unaffiliated hackers or groups that are attacking these organizations?

Terry Ray: Well, in terms of the government-sponsored pieces of it, I would say, I'm no conspiracy theorist, but I believe that, certainly, governments -- not just China, but China, Russia, the United States -- all countries have some sort of cyber-warfare, cyber-IT groups, whatever. And maybe they're clandestine, maybe they're not, but, at the end of the day, they're probably doing something now. The attacks that we've seen recently, or over the last couple of years, do I believe that they're government-sponsored? I think the governments probably are maybe looking the other way. I would be surprised, though not a lot, if the governments were actually saying, "We want you to go do this, " and instructing teams of hackers to go and do specific things.

But I think the governments maybe not encourage it, but don't necessarily enforce any sort of protections against doing it or enforcing any sort of prevention of it. What I see, a good example, I suppose, would be where we had the attacks last summer. There were some attacks last summer that came from China.

Interestingly, the attacks that we saw that came from China actually utilized command-and-control centers and command-and-control servers out of Taiwan, and used an IP-address range that were also out of Taiwan.

And we saw these and we recognized, or there was a reputation around those servers as well as the IP addresses, that it had been used by the Chinese government, as well as universities that the Chinese government is a sponsor of and a supporter of, to do these attacks.

Now, was it the Chinese government that did the attacks? Of course, they'll never admit it, but we know that those servers have been used to compromise specific other government entities within the United States and other countries. So the corollary is there, but the proof I don't know is necessarily something that anybody's admitted to at this point.

Brian Contos: Yeah. And I think it's definitely an American paradigm to have this separation of the individual and the government, where I don't necessarily think, based on conversations I've had with people, that that distinction is as clear or as prevalent in China,

Data Security in APAC

where somebody might not be working for the government but they have this sense of nationalism, that the things that they're doing are actually for the government. Such as, if China's having political issues with another country, like a Taiwan or a Japan, they feel it's part of their nationalistic fiber, if you will, to go ahead and support their country in that respect. So I think you probably hit the nail right on the head. It's hard to say, empirically, who's right or wrong, but these individuals might be working for the government but not officially for the government.

And the government, while maybe some of the information that they are able to get is valuable, isn't necessarily sponsoring them. Or the whole thing is just fully sponsored. Who knows? [laughs] And you're absolutely right, every country does have their own cyber-warfare groups, including the US.

Terry Ray: Correct.

Brian Contos: So let's talk a little bit about the Chinese attacks against Google and Google threatening to potentially pull out, or sell off their capabilities maybe, to some Chinese corporation. What are your thoughts on that? Is that a big topic right now in Asia?

Terry Ray: I haven't heard it quite frequently in Asia. I hear it much more frequently when I'm back home here in the States. But in terms of the Chinese attacks, the interesting thing is it goes back to those command-and-control servers, and the same IP-address range out of Taiwan that was identified nine months, six months before these attacks actually occurred, at least a couple of articles that I read the other day were saying that the same command-and-control centers as well as the same IP ranges were utilized for these same attacks. The attacks were different, right? They were utilizing a vulnerability or an exploit in Internet Explorer six and some other things, as well as some phishing and other whatnots. But at the end of the day, I think reputation and an understanding of where these servers come from is a pretty big indicator.

While it's not talked about frequently, that I've seen at least, in Asia, my perspective on the whole thing is it's nothing that's going to go away. I mean, this is going to continue to happen. And frankly, Google wasn't the only one attacked, right? There were about 20 companies, as far as the articles that I read, that were attacked. Many of the companies deny being attacked or say they don't share the information. But it was a very sophisticated attack, which, really, is what makes it different.

And I think that's the biggest significance of the attack is that it wasn't necessarily pinpointed toward Google. It wasn't pinpointed toward a number of companies. It was the significance of how different the attack was, in that they had created specific trojans for specific exploits, based on specific vulnerabilities within specific companies, and then did the attack, out to gather as much data as possible and pull the data back in.

And because some of the companies aren't telling us, necessarily, that they were hacked or what they were hacked or what might have been stolen, we really don't know the magnitude of it. And my personal opinion is a lot of these companies may actually have no idea that they were actually attacked and may have no forensic information for it.

And that's unfortunate, but that's the reality of organizations, to go back to one of your earlier questions, that haven't really done the best practices around data security.

Brian Contos: It's really interesting that this is such big news here in the States, and perhaps over there, it's page 10 of the newspaper. It's not quite as important, perhaps. An interesting point you made, and I've heard this mentioned before, about attacks originating

Data Security in APAC

from China being routed through Taiwan. And it's almost analogous to maybe a decade ago, where most attacks were coming from universities, not because people at the universities were attacking other people but because they were very open systems, they had high bandwidth, high storage, at least for that time, and they were being leveraged.

I suppose just blocking every Internet IP address coming out of Taiwan probably isn't the best approach. But you mentioned reputation, and being able to really discover not just who the attackers are but what their attack vectors are and then adaptively respond.

Do you think that's really going to be the solution to these types of attacks in the future, in terms of knowing your attacker, knowing their attack vectors, and having sort of this constant, real-time adjustment towards those attacks?

Terry Ray: I think it's the next step. Is it the final solution? I don't know that there ever will be, right? It's always a tug-of-war, back and forth. But I think it's the next step of being able to recognize the growing trend, worldwide, of utilizing these multi-hop attacks. So I have either a botnet, or I've got some other type of environment. But I don't want anybody to know where I'm attacking from, so I go through a proxy, if you will, what's called an anonymous proxy. So I'll go through this anonymous proxy, and maybe I go through another one and another one and another one. And I know these devices exist because I'm in the hackers groups. I'm talking to the different hackers, and they use the same proxies.

So today, while the proxies do tend to change, the reputation of a specific proxy can be identified by various different sources. And if you've got a bad reputation on a proxy, it doesn't mean that I have to block all of Taiwan or I have to block all of China.

The reality is 99.9% of the normal people in the world don't use an anonymous proxy. These devices are typically used strictly for obfuscating who I really am, and there's only certain types of people that really want to do that.

So the fear of blocking legitimate access and authorized users to things really shouldn't be a fear at all. Instead, it should be, "I'm comfortable in blocking this because I'm fairly confident, and pretty confident that this is somebody I really don't want in my environment."

Brian Contos: Great. Well, Terry, just for some closing comments here, what are some of the other steps that either government agencies or businesses here in the US can take to protect themselves against these types, and perhaps other types, of attacks that are actually targeting their crown jewels, their sensitive data?

Terry Ray: Well, the organizations in the US, as well as the organizations worldwide, everyone has a perimeter firewall. Everyone has an IDS. These are traditional perimeter-security, if you will, or network-security solutions. And there are more and more organizations today becoming more aware of data security, whether that's on the database side, or whether it's on the web applications, which is the external portal to their crown jewels. So companies today need to be aware that whether it's PCI, whether it's Sarbanes-Oxley, or whether it's just because you want to have best practices and you don't want to be the Googles or the other 19 companies that were attacked by Google, or all the other attacks that occur annually, you need to do something to protect yourself.

You've already done it on the network side. It's time to do it on the application side. And we see more and more companies adopting this practice today, but sadly, there's still companies out there that don't have any sort of security solution on their data.

Data Security in APAC

Brian Contos: Well, thank you, Terry, and thanks so much for sharing your perspectives from your extensive travels throughout APAC and Japan.

Terry Ray: Thank you very much. Thanks, Brian.

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, please visit <http://www.imperva.com> 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