

Data Security Past, Present and Future – an Interview with Richard Stiennon – Founder of IT-Harvest and Former Gartner Analyst

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.

Joining us today is Richard Stiennon, security expert and industry analyst that is known for shaking up the industry and providing actual guidance to vendors and end users. He recently re-launched the security blog, Threat Chaos, and is the founder of IT-Harvest, an independent analyst firm that researches 1200 IT security vendors.

Richard has held positions as chief marketing officer at Fortinet, VP of research at Webroot Software, and VP of research at Gartner.

Welcome to the podcast, Richard!

Richard Stiennon: Hey, Brian, good to be talking to you again.

Brian Contos: Before we get started, a little bird told me that you might have a book in your future.

Richard Stiennon: Yeah. I've been talking and blogging and writing about cyberwar for so long that I accumulated a bunch of stories. And then last year, I was up in Halifax and some guys were doing a freelance report on cyber hacking, and they got me in front of a camera. They said it was just for a couple of statements, but they had me there for about an hour and when they were done they said, "Man, have you written a book on this?" and that was the seed of the idea. So, it's been a year since then, and obviously a lot of developments. Since then, the Pentagon was owned by the Chinese, the German Chancellery was owned by the Chinese; we've had skirmishes between Russia and Estonia, Russia and Georgia, Hamas and Israel; so there's a ton there. So, yeah, that's got me going for my next big project.

Brian Contos: What a timely subject. I'm looking forward to it. What we're here to talk about today is data centric security, or data security. There are lots of ways to really address it, but when I say that term, what does that mean to you? You've been around the industry for so long, all these buzzwords and terms, when you hear "data security" what do you think of?

Richard Stiennon: Actually, when I hear "data security" it's almost like another envelope term for all security, because without data, what are we protecting? It's not like we're protecting the copper or the fiber in the ground; we're protecting what's traversing over it, which is data, and what's at the endpoints, which is data. So, just saying "data security" turns into something that's a little hard to bite off and chew, but today it's turning into the basics - let's protect the data by encrypting it and let's protect it by controlling access to it. To me, those are the two areas of data security that I've got the most hope for, and people

are actually starting to think about those things. Some of it is compliance driven, but a lot of it is driven by the reality of the threats.

Brian Contos: You mentioned encryption. Do you think some people, especially when it comes to addressing regulations, are sort of going after security from a "Hey, I'm compliant so I must be secure," perspective, and part of that is encrypting this information? Do you think it's kind of a cop-out now? They feel they've encrypted the data so everything is OK and they can move on and look at the next big thing. Is it a bit of a crutch?

Richard Stiennon: It's definitely a crutch because it's a direct response, in the first place, to California SB 1386, which says we've got this onerous disclosure requirement unless the data is encrypted, and that's all it says. You could do Rep: 13, if you're familiar with the simplest of all encryption algorithms, and you would not have to report data losses. We've got some more current laws, in particular, Massachusetts, which is going to be a little more specific about encryption strengths. And some day Congress will pass a law too, and that might actually dictate some encryption strength or encryption methodology.

But, the trouble is that it's not the data. It's great if you've encrypted the data that's just sitting on your transaction servers, so you don't have hackers from Russia come in and steal all your credit cards. Beautiful, fine, you're good there. But, as you've written about over the years, it's the insider that we have to protect ourselves against, and in particular, it's the insider that has access to that data.

I used to say that the most trusted person in our organization is our database analysts. We've got all of these access controls about who gets access to data, except for the DBA, who is this guy with a ponytail, in the back office, who can see all of the data, all day, as much as he wants, and do whatever he wants with it. He can print it out. He can put it on a thumb drive and he can email it to himself, or upload it to a massive server at Amazon that he maintains.

So, yeah, encryption is, in a sense, a band-aid, in another sense it's something that you should be doing when you can and when it's affordable.

Brian Contos: You mentioned a couple things like disclosure laws and regulations. After Enron, we just had a storm of regulations over the past years – well Enron and others. But, given the economic situation, do you think we're in store for yet another flood? So, we're going to be talking about the new SOX the new PCI, and the new HIPAA. Are there going to be a new, new breed of regulations coming - to start addressing cyber security and data security?

Richard Stiennon: I don't see anything on the immediate horizon on the cyber security front. The environment is definitely pro-regulation right now, but Congress is going to be focusing on things that are a little more direct, I guess - CEO pay, oversight. It will take two years for Congress to pass any new laws like that, and it will take another year or more of interpretation before it trickles down to both the regulatory bodies and the enforcement folks - the auditors - to turn those into new compliance requirements. But, it's definitely a new environment of more regulations, so it is coming, down the road.

Brian Contos: Do you think we're more secure than we were before we had all these regs? Does it seem like at least it's gotten security to the boardroom? I know it's being talked about more and perhaps there's a greater awareness. Would you say we're more secure?

Richard Stiennon: Not even close. So, even if the laws were real specific about certain technologies and all that, by the time they got passed, they'd be talking about protecting

against threats that were two or three years old. So, you could imagine that Congress could get around to passing an anti-spyware bill right about now, when, you know, that's the old stuff. You can't pass regulation that's going to protect you from an attack from overseas or even an insider attack. So, I don't hold with regulations ever doing anything to support better security, other than one, and it's not a regulation. It's an industry consortium between VISA and Master Card and Discover, who came up with the PCI standards. And those have teeth in them, to some extent, but I'm sure that we know that TJX was PCI compliant. They had passed their compliancy requirements. The most recent disclosure of now over 100 million credit cards probably lost with this company out East, the same thing. They're probably PCI compliant in the app, and they're totally hacked. So, the PCI requirements don't even protect your data very well.

Brian Contos: I read a great blog entry from somebody who you might know over at Qualys right now, he used to be at LogLogic, Anton Chuvakin.

Richard Stiennon: Oh, yeah!

Brian Contos: His blog entry was great. It was basically "You know, the Titanic was actually complaint." [laughter]

Brian Contos: He went into this story how it was compliant, but the regulations were dated. They were actually for ships that were a much smaller size, and they never rewrote the regulations. So, the Titanic, clearly being a much larger ship than its predecessors, did have the required number of life boats. It was fully compliant, but as of course we all know it didn't work out too well.

Richard Stiennon: That's great! Like the story of the... They called in an efficiency expert, because they wanted him to analyze how we could better fire cannons, leading up to World War II, their artillery. So, this guy is watching them and he's scratching his head, because it's like four guys assigned to different aspects of it. Right before they pulled the linear to fire the gun, one guy was stepping back like 20 paces and just standing there. That was in the regulations, "This is exactly how we do it. We're not compliant with our own regulations if this guy isn't there to do that." They searched around and they finally brought in an old guy from pre World War I, and had him watch how they shot off those artillery. They asked him, "So, what's this guy doing when he steps back?" He goes, "Oh, he's holding the horses."

Brian Contos: [laughs] It's amazing! I think, that's sort of the false sense of security that a lot of these organizations fall into with that. I think compliance did a great job. I think the industry consortiums, you mentioned PCI, there's also NERC. They sort of get the information out there. They get the conversation out to a more senior level, but sometimes they just don't get the essence of security. It's the "Letter of the Law," not the essence of the law, if you will. It's an interesting dilemma, and you're right. I completely agree with you, I am not sure government is the answer for that either. So, let me ask you, getting back to data, and sort of databases and application. Most of us that come from a network security background, we think of firewalls and IPSs, and things of that nature, VPNs, but when you're talking about databases and applications and business process transactions, that was always the other group.

It seems like these two things are merging now. Do you think there's going to be sort of this new generation of security professionals that are network folks? They're security folks, they're application folks. They've got all of these skill sets, it seems like something difficult to consume.

Richard Stiennon: Yeah, I can't say that I've bumped into people like that. I think it will come from people that do security around new application developments. So I'm sure if you went to Amazon, eBay, and met with their security people, they would be ones who do take that perspective of looking at everything from the network, application, data, and people side. Even somebody at Yahoo or Google Gmail who is just watching the flood of ways that people scam their systems and take advantage of their user base, they're the ones that have to think in those broad terms.

Brian Contos: Yeah. I heard the analogy the other day that, "Data centric security is today, where perhaps network security was in the late 1990's." It's basically the 'wild west,' because there is somebody armed with as little as a web browser that knows where the apostrophe key, can create quite a bit of havoc. It's cross-site scripting, it's SQL injection, and there's just a number of threats out there. Then you get into these more advanced things like these cross-site request forgeries, CSRF, and some of these things. It just amazes me that the applications and the databases have almost evolved in this vacuum. Now that their front ending business processes via web browsers or they're part of some type of SOA architecture, they're extremely vulnerable because they're not in the back office anymore.

I think we're going to see, my prediction - I know it's January, 2009, so everyone is making predictions, but my prediction is for 2009, we're going to see a lot more application and database focused attacks.

Richard Stiennon: Yeah, no question. On top of that, we're going to see the user credential attacks. So, all of these guys have rolled out these great applications, and they say, "Well, it's just for my customers, so I don't have to send it as strong as I would if it were open to the public and hackers from Russia." They're going to run into the same problems that LexisNexis ran into where the customers will understand the application and how to hack it, and run dictionary attacks against user names and break in and use it. You can't trust anybody.

Brian Contos: You can't trust anybody, boy! When you're designing security, when you're designing these applications, I think it's absolutely right. You've got to take into consideration like you mentioned before, malicious people that also potentially have the keys to the kingdom, not just the un-trusted outsiders. From that perspective, it really makes you rethink how you're approaching security, doesn't it?

Richard Stiennon: If a trusted insider has keys to the kingdom, how well are they defending them? Right now, a textbook case is Twitter, where some random hacker heard about Twitter somewhere and happened to pick somebody's ID to try and crack. He noticed right away that there were no limits on password attempts for logins. So, he decided to run a little script against a particular user ID, which just happened to be a support person at Twitter. From there, he got into the password reset facility exposed over the web. I am sure it was at Admin.Twitter.com. He started stealing accounts from Barack Obama's campaign, and Brittany Spears, and Fox News, and it could have been a disaster.

Like two months before, they pointed out how vulnerable they were to that kind of an attack. Luckily this kid wasn't reading this blog, so he couldn't point to it. So, he learned it from Stiennon.

Brian Contos: [laughs] On that note Richard, let's sign off now. As always, it was an extreme pleasure having you.

Richard Stiennon: My pleasure.

Data Security Past, Present and Future with Richard Stiennon

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