

PCI, Security Blogging & Podcasting – an Interview with Martin McKeay – Host of the Network Security Podcast

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 Martin McKeay. Martin started blogging about security in August of 2003. He took up blogging as a means to expand his knowledge and test ideas about security, by putting them up for peer review. Four years later, he's still at it. He works as Senior Consultant for Trustwave, specializing in PCI assessments as a QSA. He has a podcast, co-hosted with Rich Mogull of Securosis. He also writes for Computer World. Martin's Network Security blog and Network Security podcast are among the most read and most listened to security resources on the Internet today.

Welcome to the show Martin!

Martin McKeay: Thank you for having me, Brian!

Brian Contos: You know, Martin, we were just chit-chatting before we started the recording, that you were actually one of the first podcast interviews that I ever had, back when I wrote my first book, "Enemy at the Water Cooler" and I was looking for some security podcasts out there to talk with. That was a couple of years back--but since then, boy, your podcast has really taken off. Could you, maybe, share with the audience some of the stats and figures around the Network Security podcast and blog? I think they're really quite impressive.

Martin McKeay: Well, I mean, it's the Internet--so stats are always a little bit questionable. I think nowadays, Rich and I--Rich Mogull is my co-host--are getting around anywhere from 2,500 to 3,000 downloads per episode. I think the blog is several thousand hits a day. And you know, I'm getting out there and really letting people know I exist, and letting them hear my voice on a regular basis.

And I have to be honest--yours was one of the first real interviews I had done as a podcaster. Since then, a lot of interesting people, and a lot of interesting stories have passed my way. It's been a lot of fun.

Brian Contos: Well I've been an avid listener, so I'm happy to say that "Martin McKeay Podcast" shows up on my iPod quite frequently. Martin, I know yesterday there was the house sub-committee on PCI, and they actually did a live webcast of that. And you were able to attend. Can you tell me a little about what this was, first, for if some of our listeners didn't get a chance to actually view that?

Martin McKeay: Well, basically, the house sub-committee--and I'm not going to try and say their whole name, because it's really long--they were saying: do the PCI standards work in reducing cyber-crime? And I think that they kind of went in with the assumption that PCI

isn't working, and that something else needs to be done to further secure our businesses, and our credit card numbers, quite frankly. I was a little surprised, because the Department of Justice Representative--and I forget her name also--kind of sat there and said: you know what? PCI is not the be all and end all of security, but it is a good round port. It's a good base level for merchants to comply to.

Then they had Bob Russo, because he's the head of the PCI Council, and a representative from Visa itself. They had a representative from Michaels--a merchant--and somebody from NFR, which is National Foundation of Retailers, I think.

And it was very interesting to watch. Bob Russo, obviously, is sitting there and defending PCI, and say: look, we're doing a good job. Visa is sitting there going: yeah, PCI is making a marked improvement.

On the other hand, the merchant and the representative from the NFR Council, is saying that there's a lot of problems with PCI and there's a lot of information that is kind of muddled.

So I think, overall, maybe they took more of a beating than they gave--"they" being PCI and Visa. But, overall, I think, they did a good showing, and I don't think this is going to be the last that we're going to see of them up there.

Brian Contos: Was there anything, that you would say, is shocking, or game-changing, that came out of that? I mean, a lot of people out there say PCI is not a silver bullet. It's a good start, it gets people talking about it, increases awareness. It takes some security measures to at least a common baseline. Did they come out and say anything that just looked like it came out of left field?

Martin McKeay: No, I think a lot of these arguments have been solidified over the last three or four years. I think one of the comments that was made is about moving to a chip-and-PIN architecture, or moving to a tokenization architecture, for online transactions. And I do think that Visa, and Mastercard, and the PTA Council are looking at that.

But Bob Russo made a good comment about those that allowed encryption--if the PTA Council makes those part of the PCI standards, there's a lot of merchants who aren't going to be able to afford to make the changes in a timely manner. And if they can't make those changes, they're not going to be compliant, and therefore they're not going to be able to do business.

Brian Contos: Martin, getting back to you and the blog, and the podcast; clearly, you're one of the most seasoned security bloggers and podcasters out there today. Certainly the most consistent. What are some of the changes that you've seen since you've started in the security industry as a whole? Maybe, what are some of the problems that were there at the beginning, and they still remain?

Martin McKeay: Yeah, I guess I have been around a little while--I think I've been blogging for five and a half years, and podcasting for almost three and a half... It's kind of hard to distinguish between what the security industry is doing and what I've been doing as a security practitioner.

I think, in both cases, that we're seeing a maturation of the security profession. I think that we're starting to realize, more and more, that security professionals can't just be computer geeks who specialize in firewall rule sets. They have to be people who understand business

practices, and can talk to the CEO and the C-level execs on their level and make them understand why security is beneficial, and why they need to pay attention to it.

On the other hand, they also are learning to listen better, too, and not just say "No, you can't do it." But to say, "OK, if we are going to do what you need to do, here are the risks that we're going to take." And I think that that's a really good thing for the security industry to do, as a whole.

Brian Contos: Definitely. When you're--at least when I'm out there in the field, as well--talking to organizations and security practitioners, there's much more business relevance to what I'm seeing being done. I think that's one of the reasons why you're seeing this cross-over now, between traditional IT security, and fraud, for example. Especially as application database security became more entwined with traditional network security. So, I think you're absolutely right. I think there's more business DNA being involved.

Not that the guys writing code, and hacking away on things, and finding vulnerabilities, and discovering new ways to protect against those vulnerabilities, are going away. That's absolutely a necessary part. But from an organizational perspective, it's a good thing--it's much more aligned with organizational business processes, and business risk. Which I believe is a positive thing for our industry.

Martin McKeay: The other thing is, is that businesses are starting to realize, more and more, how important security is to get involved in earlier in the process. It's no longer something that you can just tack on to the end--which is, quite frankly, how a lot of businesses used to think about it. Now, they're beginning to realize that if we want to make our processes secure, you have to think about it from the beginning. We've still got a long way to go, but we're doing a lot better than we were five years ago.

Brian Contos: Maybe you're seeing this as well, but I'm actually starting to see, now, that the person tasked at a strategic level with organization security--while it's still very common to see that be a CSO, or somebody reporting up to the CIO--more and more I'm seeing that move over to its own independent group, reporting up to, maybe, the CFO, or in some cases, even the CEO, or Chief Compliance Officer, Chief Risk Officers. So it's not just going up that IT path anymore, and I think that makes a lot of sense, because sometimes there's conflicting agendas there.

Martin McKeay: Well, the other half of it is, the bad guys have matured a lot too. When I got into it, the bad guys were still, for the most part, just somebody hacking away at a computer at home. Now, they're organized crime, and it's big businesses. The myth that it's outstripped the drug trade, it's pretty well debunked--but it may be there, at that level, in five years.

Brian Contos: You're someone that's been involved in various forms of standards and regulations--certainly, you're a QSA, so of course you're very up to speed on the latest and greatest around PCI, for example. Overall, do you feel that the standards and regulations, as a whole, have hurt?

Martin McKeay: I looked at PCI, and I looked at the business I was working at, and I realized that PCI was the baseline that we had to meet. And even getting to that level was going to be hard. I was able to turn around and use the regulations, the standards, that are PCI. And use that as: no matter what you say, no matter what I say, here are the minimum requirements we have to meet. Otherwise, we're not going to be compliant, and we're going

to pay for it. And that's a big stick for security professionals. It's no longer my opinion, or your opinion--here are the standards, here's what we have to meet.

And yeah, I think that if you can get the majority of the merchants meeting something like PCI, or any of the other standards, it's probably going to raise the security of our environment overall, significantly.

So yeah, I think that regulations and standards hurt.

On the other hand, they're not risk based, so they don't necessarily apply to your company. It's just a checkbox, or a list of checkboxes, and that's an improvement that we need to see on there.

But I just don't think that businesses are even hitting the bottom line yet, let alone going beyond it to actually addressing the risks in their corporations.

Brian Contos: Sure. So it's certainly not a one size fits all type thing, and I think that's what a lot of organizations are struggling with, right? They're saying, "We have certain mitigating controls and processes in place, and other things that don't necessarily map into what the standards and regulations say." And it can sometimes make it difficult to get through an audit.

Martin McKeay: And when you add in the government, and some of the SOX and other requirements there, and things get really murky really quick. And we're living in an environment that's constantly changing, and sometimes the standards have a hard time keeping up. That's one of the failings.

Brian Contos: So Martin, given the overall economic crisis, how do you think that has impacted security? Or perhaps, how do you think it's going to impact security?

Martin McKeay: In a lot of cases, I think that it's not affecting security--or, at least not yet. I think that, again, to specify PCI--it's not an option. It's not something you can say yes or no to. It's something you have to do. And therefore whether there's an economic crisis or not, you're going to have to meet with those standards, and lot of those businesses are finding it kind of hard.

I think we are probably going to see some downsizing in the security market, and security vendors, because of this. And maybe some of the ones that have a hard time meeting with compliance, some of the merchants who have a hard time meeting with compliance, are also going to be gone over the next couple of years.

But as of this point, I haven't seen too big of an impact, or heard of too big of an impact, in the security sphere.

Brian Contos: I'm asked that question quite often, and honestly, even with financial organizations, which you'd think would be seized up more so than anybody else... Sure, budgets, in many cases, are being stretched pretty thin, but overall--because of layoffs, because of the economic crisis, because of various problems in the organization--it seems like they're taking a more programmatic approach to security. Especially as it relates to things like insider threats--and threats potentially from consultants and contractors that have been let go, or employees, or possibly partnerships that have gone south. And it seems that there's an increased awareness and pressure to add security controls--specifically around those types of threats.

Not that perimeter threats and other things have gone away, but that definitely seems to be up-ticking, at least from what I've seen.

Martin McKeay: I tend to agree with you. I think that people are beginning to realize... I don't think it's necessarily related to the economy. I think it's related to awareness, and over the last few years, awareness of some of those threats and why we have to worry about them, has really risen. Especially with all of the disclosure laws, and the fact that, I think 49 out of 50 States have some version of a disclosure law. If you're compromised, you have to tell everybody about it--there's no ifs, ands, or buts.

That hasn't resulted in anybody having major problems yet--since, I think, CardSystem, but it still is embarrassing to a lot of companies to have to admit that they didn't have enough security in place, and that's why they got hacked.

Brian Contos: With SOA, a lot of very complex application and database infrastructures, that are being front-ended to the Internet, that there's never before been so much information exchange exposed to the outside world--or potentially exposed, as well. So even though I'm a big proponent of saying you need security controls specific to individuals that you may consider insiders, I think given the way architectures are going, a lot more people are probably considered insiders... [laughs] ...when you take into consideration how much information they have access to. Either directly, because they're supposed to, or possibly indirectly because of mistakes, or bugs, or flaws, or something like that.

Martin McKeay: And then you add in the big buzz word in the industry right now--cloud computing--and well, where is your data in the cloud? It's just like the Internet cloud, where your data goes in, and you don't know how it gets to that site--but it gets there somehow. The cloud is the same way. Yeah, my data is on Amazon's server somewhere; I don't know which servers, I don't know who is else is sharing those resources. I don't know what else is attached to those. It's a real big thing that we're really going to have to watch and make some big decisions about over the next couple of years.

I've watched what Chris Hauth writes, and you know, cloud computing kind of scares me - especially as a PCI assessor--because I don't know how many people are going to start looking at that and just assume it's safe, and start moving in that direction whether it's the right way to go, or not.

Brian Contos: Whatever direction you look at, whether it's virtualization, SaaS, cloud computing--whatever terms, verbiage, you might use--the bottom line is, there's so much buzz about it. Just about everybody is talking about it, whether they want to get involved, or how it can save them money, or how it can cut down on data set-up costs, et cetera. And I think that leads into my next question for you: looking into the Martin McKeay crystal ball, what are your predictions for the next big trends, or problems, or mitigation techniques in, let's say, the next five years?

Martin McKeay: Global economic meltdown--no, I guess that wouldn't be right.

Brian Contos: [laughs] Thermo-nuclear...

Martin McKeay: Yeah. Cloud computing's going to take a couple of years to really hit a point where we've figured out what's OK and what's not. I think that, at least for the next year or two, is going to be our big discussion, and our big talking point.

PCI, Blogging, and Podcasting with Martin McKeay

I think that PCI is still figuring out what its legs are, and where it really sits. I think that that, for at least another two to three, maybe five years, is going to be something people are stretching to comply with, not an accepted baseline. So I think that's a big thing.

Other than that--you know what? I think, if anything, we're going to see more of the bad guys becoming organized. I think we're going to see more of the good guys becoming organized. And maybe some more inter-industry communication.

But anything other than those few things, it's almost impossible to predict more than three months out, let alone five years.

I think a lot of the things that we accept as basics, are going to remain the same, and always will. What form those take--whether it's cloud computing, or visualization, or something else that we haven't thought of yet... If I can predict that, well, then I'd be called Richard Steven.

Brian Contos: [laughs] What closing comments do you have for our audience, today?

Martin McKeay: Well, I'm working on an interesting project right now. I'm going to be the podcast sponsor for the Forum of Instant Response and Security Teams, in Kyoto, Japan, this Summer. That means that I'm conducting some interviews leading up to FIRST, that I'll be publishing, and just talking to people who are going to be giving keynote speeches there. I'll also be doing some podcasting from Kyoto, Japan, and it's my first time in Japan so I'm really going to enjoy that.

There's the security bloggers' meet-up at RSA later this month, that I'm one of the hosts for. And that's going to be a lot of fun. Tthis Summer, and maybe actually spend some time with my family.

Brian Contos: Martin, as always, you are busier than anyone would ever expect one person to be. [laughs] So, I thank you very much for being on today's show.

Martin McKeay: Thank you for having me, Brian.

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.



