

## PCI and Data Security – an Interview with Dr. Anton Chuvakin – author and recognized security expert with Qualys

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](http://Imperva.com), check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at [blog@imperva.com](mailto:blog@imperva.com).

**Brian Contos:** Joining me today is Dr. Anton Chuvakin. Anton is a recognized security expert and book author. He is an author of the book "Security Warrior" and contributor to books such as "Know Your Enemy II, " "Information Security Management Handbook, " "Hackers Challenge 3, " and "PCI Compliance." Anton has published numerous papers on a broad range of security subjects, and in his spare time he blogs at securitywarrior.org. In addition, Anton has presented at many security conferences across the world. He has recently spoken in the United States, the UK, Singapore, Spain, Canada, Poland, the Czech Republic, and Russia. He holds a PhD from Stony Brook University.

Welcome to the show, Anton.

**Dr. Anton Chuvakin:** Thank you so much, Brian.

**Brian Contos:** So Anton, before we begin, I always like to ask my guests, what is it that you've been working on?

**Dr. Anton Chuvakin:** OK. In my case, that's pretty easy. Lately, I've been involved with PCI DSS compliance. And as we know, there's no single technology that addresses all the needs, or even the majority of the needs, of PCI compliance. So I was involved with Qualys's efforts to build a PCI platform to do more things around PCI compliance. I wouldn't go into too many details, but it's like you're tying different solutions together for helping merchants comply with PCI, as well as for helping banks and the client organizations to check the status of those merchants. So it's really the story is about PCI and making PCI easy for merchants and for a client base, while obviously manifesting all the security benefits of PCI.

**Brian Contos:** Yeah. You know what I always find interesting about PCI as a general topic is, whenever you're talking to an organization about any other type of reg -- you're speaking to them about HIPAA, Sarbanes-Oxley, GLB, even NERC -- a lot of them relate things back to PCI as sort of the right way to do things.

**Dr. Anton Chuvakin:** Well, the reason for this is actually somewhat different, in my view. It's not so much that it shines, as far as being called. It's more due to the fact that PCI is just so much more prescriptive than other regulations. And as we've learned over the years, it seems to be easier for people to deal with prescriptive regulations, compared to the regulations that mandate the end results. In one of my blog posts, I was trying to address the concerns some people had with PCI, namely the criticism that PCI is actually too prescriptive. I don't agree with that. I think PCI is prescriptive enough. In many areas, we

## PCI and Data Security with Dr. Anton Chuvakin

can even clarify some of the things. In my view, that's the key for PCI's popularity as a reference standard, because it has the details filled out.

Now, some other regulation might call for you doing the right thing to manage risks, and then your organizations have no idea what's the right thing for them or for anybody. So PCI does explain that it has sort of its policies, standards, deploying technology, vulnerability scanning, and other things. And so I think that's what drives that option of PCI as a back-end framework for many other things.

**Brian Contos:** And I've seen a lot of people try to address IT governance, leveraging NIST 800-53 controls, for example, or ISO 17799 for higher-level business objectives on top of that. And it's a massive, massive gray area. Take NERC for example: "Protect your critical cyber assets." What's a critical cyber asset, and how do I protect it? [laughs]

**Dr. Anton Chuvakin:** Exactly.

**Brian Contos:** Are we getting better? Is PCI making a difference? Or what's really been the outcome? It's been around for a while now. People have implemented it. People have become PCI validated and a number of other passing criteria. Is it helping?

**Dr. Anton Chuvakin:** Here's the thing. When people say things like "It's been around for a while," "It's been adopted," "People have implemented this." Actually, what I like to use as a focus is a bit of an unusual angle here, namely, what people are we talking about? Specifically, I think PCI's biggest positive impact -- and I think that it has a huge positive impact -- was for those people who would not have done anything otherwise. Now if you have a security program, you have a CSO, you have a well-managed security-technology unit and the sort of softer ethics of information risk management, I mean, PCI is helpful to maybe structure some of your efforts, but it's not going to make huge improvements for your security because your security is already at a really good level, and you know where it should be, and you steer it there. So PCI becomes very easy for you.

However, that's not the point of the PCI DSS. The point, to some extent, is to make people who really cannot stealth security to become more secure so that their credit-card numbers that are present in their organizations are better protected.

So I think PCI's huge impact was at the very bottom tier, where people who would otherwise do exactly nothing, their top security measure would be certain top-brand anti-virus with an update that's expired three years ago, that type of stuff. And for them, PCI is the much, much needed kick in the butt that makes them do security, makes them first think about security, understand security. To some extent, not sort of a great depth. And this is where I think the biggest positive impact is.

**Brian Contos:** Yeah. I've actually heard it referred to, occasionally, as it gets people to the actual starting line, so they can really begin working on security.

**Dr. Anton Chuvakin:** Correct.

**Brian Contos:** At least do this so you're not blatantly open and exposing credit-card information and just giving up the crown jewels. Once you've done this, then you can actually really work on true security throughout your organizations.

**Dr. Anton Chuvakin:** And as you've broken PCI, you actually figure out what this is, because if you tell many of those companies, "Hey, learn security and do it," they will really just give you a blank stare and that's all there is to it. Now, if they have gained experience

## PCI and Data Security with Dr. Anton Chuvakin

with PCI, at some point they start thinking, "Oh, PCI is awesome here and here, and we finally are getting our risks under control. But how about this other area? Oh. OK. We need to address it." And so they really educate themselves, using PCI. And so they start thinking about closing other holes and closing other things before it happens.

**Brian Contos:** What do you think is the most misunderstood issue regarding PCI?

**Dr. Anton Chuvakin:** Interesting, because right before this call, I was actually creating a mind map of all PCI mistakes and misconceptions, and I still have this HUGE chart open on my screen. [laughs] And I'm looking right at this, and I've already put about 25 items of different PCI myths and misconceptions. And suddenly, Brian's asking me to name one. [laughs]

**Brian Contos:** You didn't know that I had a keylogger on your system, did you? [laughs]

**Dr. Anton Chuvakin:** No, I totally did not. I was completely oblivious to the fact. But then again, nowadays everybody's owned, so I'm not at all surprised. [laughter]

**Dr. Anton Chuvakin:** So, if I had to name one myth. Hmm. OK. Something tells me to name this one. We are so small, and we can hide under our desks and wait until PCI goes away. I think that's the biggest, most dangerous and truly one of the most dumb misconceptions about PCI, because the fact that you are small and the fact that you don't know security now and don't want to know it does not make PCI any less relevant. In fact, you are the person PCI was written for, and there is no way you're hiding under your desk from it. And maybe you can hide for now, but there's no chance that you'd be missed at some point.

**Brian Contos:** Yeah. Just because you close your eyes and go under the pillow, it doesn't mean that the monsters in the closet actually go away.

**Dr. Anton Chuvakin:** That's correct, yes.

**Brian Contos:** On my side of the house, with Imperva, we talk a lot about web-application firewalls and database-activity monitoring. And there seems to be this thread of debate, when it comes to PCI, of what's needed and what's really the best solution. Is it WAF versus vulnerability scanner? Is it a combination of WAF and vulnerability scanner? Being that you're at a vulnerability-scanning company, and I'm at a WAF company, what's your perspective on that? And I'll tell you mine very quickly. I always believe that defense in depth is the way you need to go, and it's a combination of multiple tools, tools that can do discovery and analysis and prevention and detection and response. So I think it's a combination. But I really wanted to get your honest opinion. Where do you fall in the sort of WAF and vulnerability debate?

**Dr. Anton Chuvakin:** Well, I think it even starts before you even thought of the words "defense" and "depth." Because I think, before you say defense and depth, you have to say common sense. And if you think about physical security as something... I mean, even not saying anything as grand as physical security. Think about your own house. Would you really debate things like, "Do I need a door, or do I need a lock? Do I need to close the door or windows? Do I need just a ban? Can you go hide guards or cameras or locked doors, or have an alarm system?"

I mean, if you try to use this analogy -- and we all know analogies are not perfect -- you really come up with pretty darn idiotic phrases. "Locked our doors" has happened. And then, if you take it to an even more advanced level, you start thinking about, "Do I need to

## PCI and Data Security with Dr. Anton Chuvakin

secure things, monitor things, or do I need to assess them?" Gee, you need all three. You need to assess, secure, and monitor. There's no way that you just put a lock on a door and then say, "Oh, well, the rest is not important."

So, this is not just defense and depth. This is just common sense telling us that you need both, in this case, because you need to assess the security posture, you need to block attacks, and you need to monitor. There's really no avoiding all three.

Hey, Brian, did you really expect a debate on this?

[laughter]

**Brian Contos:** It's amazing to me, to be quite honest, how many people out there just feel that code review or vulnerability scanners are the way to go, and simply write better code, forget about controls on the outside. To me that's like saying, "Just go ahead and build a car that never breaks down."

**Dr. Anton Chuvakin:** Oh, but that's nice, right? Isn't it nice?

**Brian Contos:** [laughs]

**Dr. Anton Chuvakin:** I mean, I could totally buy a car that never breaks down. And I would get an app that's written with the best advances of the 23rd century SDLC, and it's just secure. Sure, that's cool. But where do you get that?

**Brian Contos:** Yeah. I haven't seen any of those on SourceForge.

**Dr. Anton Chuvakin:** [laughs] Not lately.

**Brian Contos:** [laughs] Well, that sort of takes us in another direction as well. When you're thinking data security, or I should actually call this application and data security, a lot of people talk about, "Well, you really need to protect the web application," and some people say, "No, you really need to protect the back-end database." I think it's the exact same argument. When you're talking about protecting your data, whether where it's being processed at the application, or where it's being stored within the database, sometimes the same physical machine, it's really a question of sort of common sense, to your earlier point, as well as defense and depth monitoring up and down that stack, isn't it?

**Dr. Anton Chuvakin:** I mean, in my view, the data-security debate or the data-security conundrum is just a whole universe of things. You can't even compare, say, data security or replication security to things like network security, because a network is a pretty specific thing. You can point at a router and a bunch of wires and servers, and network is something which is much easier to visualize. But try to visualize data. Data is just so amorphous. It's everything from a post-it note on your screen -- that's the one with the password -- and databases and files and desktops and mainframes. So data security is just such a universe of things that trying to say "What's the solution to data security?" is maybe even more complicated than trying to say "What's the solution to world hunger?"

So technologies like the ones you mentioned will certainly help. I mean, there's not even a clear framework to think about data security for a large company.

**Brian Contos:** The notion that there is some type of silver bullet -- years ago, some people thought it might be encryption: "Encryption will save us all." And I've had some encryption experts on this program as well, and they all agree today that by no means is

## PCI and Data Security with Dr. Anton Chuvakin

encryption the savior when it comes to application and data security. It's one piece of the puzzle, for sure, and I think it's necessary in many cases. But so is access control. So is auditing. So is vulnerability scanning and assessment. I think it's really just going to this notion of the maturity of security in our industry. What we talk about when we're talking about information security today - and, Anton, this is a great one to get your perspective on as well -- is it's so much different than how we thought about it, or at least most of us, or at least me, how I thought about it 10 years ago.

**Dr. Anton Chuvakin:** That's true to some extent. But I guess we can't really say that it's truly business-focused yet, because it would be some kind of a security nirvana, where there's exactly enough security to run a business well. To be honest, I don't think we're at that level. We are sort of at the level of getting enough security so that everything doesn't just fall on us, which is not the same as saying we have enough security to run businesses well. And encryption is actually a perfect example. I do think encryption is a solution to all the security problems, as long as you encrypt the data and throw away the key. And so security-wise, certainly the data would be protected. And it's the good old concrete-cube security model. When you get a computer, just pour some concrete over it and then sink the resulting concrete cube. Someone else will definitely be protected.

And how do you balance this type of security with business is actually much more of an unsolved problem than any zero-day protection technology we can think of.

And in light of this, I'd like to mention one of my recent favorites in security: namely, security metrics. How do you measure what you're doing with security, and whether you're doing enough, not enough, whether what you're doing is cost-effective for your organization? And please don't say ROI. I hope you wouldn't. But having an ability to measure security in an objective way is probably the biggest advance that we have not made yet on our road to security and information risk management.

**Brian Contos:** With that, Anton, what final comments do you have?

**Dr. Anton Chuvakin:** A final comment I would like to make is that it's really fun to talk about subjects like security metrics, ITGRC, encryption, data security, web-application scanning, and all these really cool technologies that are very useful. However, when we talk about this, and then we sort of play the industry visionaries on TV, we need to think that there are organizations out there that are confusing firewalls with fire extinguishers, today. And those organizations handle credit technology. That's your credit card numbers and my credit card numbers. Well, technically, those are banks' credit cards, but that's a separate point.

When we think about any and all security/technology advances or innovation in the domain of policy, we have to remember that there are millions of organizations that are still not quite at the level of updating their anti-virus encryption. And I encourage any and all security professionals to remember that those organizations exist out there, and they have access to our data.

**Brian Contos:** Well, Anton, thanks so much for joining us today. It was an absolute pleasure speaking to you again.

**Dr. Anton Chuvakin:** Thank you so much.

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