

Cyber Crime, Data Security, SOX and PCI – an Interview with the 451 Group's Nick Selby

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 Nick Selby. Nick leads the 451 Group's Enterprise Security Practice, or ESP, which provides objective analysis of enterprise security businesses and trends. Nick also serves as the 451's Director of Research Operations, leading the coordination of the 451 analyst research methodologies and processes.

Welcome to the show, Nick.

Nick Selby: Hey, thanks, Brian.

Brian Contos: Before we get started and get really deep into the questions, I know there are a number of things that you've been working on lately. If you could, let's maybe just spend a couple of minutes talking about some of the latest and greatest.

Nick Selby: Sure. I'm not sure how great it is. We're working on a fairly large report which updates our 2006 report on security information management. What we're doing is going back to take a look at some of the larger deployments that we took a look at two years ago and bringing in whole bunch of new SIM customers - people who bought a SIM product over the past couple of years - to see how expectations and requirements on the customer side has evolved over the past couple of years.

We have some theories around where the markets going, so we're testing it to try to see whether they're right and if they are, what it actually means for the SIM space where those vendors in that industry are going.

We're doing quite a bit of work on the information protection and the evolution of the typical data loss prevention technologies like anti-data leakage, encryption, device control and database transaction laundering.

We're seeing how those are being put into a much more holistic look at information protection, both for the commercial sector and in government. So this is better integration of identity and access management entitlement and access control, more visibility into data in the enterprise. How data's moving, what's normal and what's not.

We're also looking at dynamics between investment in compliance and access control. When did the tactical compliance automation project become actually a strategic investment in policy driven access control?

We're looking also a bit as identity as a service of this as Cloud Security becomes more and more something that people talk about - and as of course, the economy pushes people to looking at services and security as a service.

How far can we take this? Can we actually do identity as a service? How is that shaking out for the people who are trying that? Who are the kinds of customers who would buy that? What is it that they're looking for? What will they be looking for over time?

Paul Roberts is doing a lot of work on social software and social networks and the convergence of that and web and application-based attacks and the way enterprise security issues have been mirroring consumer security issues and social network security issues. That's bringing us into the biggest thing on our agenda for this year, which is online crime.

We're not looking at really at attack vectors and exploits. There are a million people who look at that. We're really trying to get a better sense of the business issues from the standpoint of if these are the large criminal organizations that we know are conducting a lot of the crime that's online - if this is a really organized thing - how are these businesses run?

What are the business models? What are the R&D models? What are their milestones and deliverables? How do they select targets? How do they decide what it is that they're going to go after, in terms of different organizations or different applications?

How do they create and sustain demand for what it is that they're doing and resell things that they're doing? So looking at the business of Internet crime.

Brian Contos: That's fascinating to hear your point. There's so much work being done on the attack vector side, but people usually just make an illusion to the black-market, the underground economy. But no one's really dug into it as far as I know, the story behind this, or....

Nick Selby: Sure.

Brian Contos: ... are these loosely fitted organizations? Are these government sponsored organizations? Where do they get their funding? How do they define their targets? I think that should be a really fascinating study. When do you think information around your research in that area will be available?

Nick Selby: It's probably going to be start coming out in the April timeframe, leading to a fairly large report that we're going to be releasing in June. But I would say that's the biggest single issue on our research agenda for this year. As we look at all of the different smaller issues around enterprise security in 2009 as a security practice, we're really looking at those things and in the context. Not just as of protecting enterprises, but defending against increasingly organized, increasingly sophisticated attacks.

And again, not looking at there's this worm or this particular exploit that's come out. But more along the lines of what are the things that I can do to lower my attractiveness, generally? How are targets selected? We think that that's going to be really, really fascinating.

Brian Contos: So, Nick, with that, you get exposed to so many different end users and different vendors globally, what are you seeing as really the big trends in security and also trends around compliance? What's happening out there?

Nick Selby: I think it's boring to say, but I do think that the biggest single trend that we're seeing is security becoming more and more about operations, more and more about risks, and that's been the case for some time. I wish I could say something that was much analyzed in and very buzzy, but I really can't. I think that the repercussions of people beginning to look at security like this and weigh security investment decisions and security posture against an overall understanding of risk and a better and more detailed and granular understanding of risk.

I think that that's a really fairly large trend that's going to continue to shake its way out over the course of certainly this year and next year. There are a lot of issues just around that understanding and changing the mindset.

If we can't do this because it's bad, what's the worst that could happen if it did happen? What's our business risk? How does this affect our shareholders? How does this affect our value? How does this affect our ability to take information and turn it into something that we sell? We don't underestimate the repercussions of this trend.

I think in terms of compliance then that the first trend sort of feeds into the second one. If you remember, around a couple of years ago when banks were gearing up and they were dealing with online fraud issues.

They were racing to comply with requirements from FFIAC to have more than single factor authentication. I remember a fascinating conversation I had with my bank, because they didn't actually do anything until March. I think the deadline was December 31 you had to have it done.

What they'd done was they had done a risk analysis. They said, "Well, it will cost us a few hundred thousand in fines and we'll make X million dollars. In the meantime, the price will come down and we'll make sure that we have absolutely the right protection." I think that we're seeing the follow-on of that in compliance.

We've seen PCI as a really smartly written - a very, very well written standard. It's prescriptive, it's descriptive. We were just over at PCI today talking with them about how they're going even farther to make the intent behind each subsection much clearer to the stakeholders and to the merchants who have to deal with this, and to the auditors.

And what you have then is you have compliance. And you have regulatory rule sets and industry rule sets that don't leave as much up to interpretation from, for example, your auditor. You actually make people have a better understanding of what it is that they're expected to do for the goal obviously, or becoming more secured, not just merely compliant.

And we've seen this happening over several years. And we think that it's going to continue that regulations and industry rule sets are going to be better written in order to better communicate the final intent and not just the letter of the law.

Brian Contos: When a lot of people think about PCI, they definitely, because it is so prescriptive, they see it as really a foundational standard that other standards leverage. I know that NERC for example, something for the North American Electrical Reliability Corporation, and how they look at the electric industry, it's a little bit more in the gray area. To me, it feels a lot more like Sarbanes-Oxley, a little bit more like HIPAA, than it does like PCI. And I always feel like PCI, the direction they took is really the direction to go.

But one thing that I have the fear of, and I think we all agree with this is that these standards, these regulations, what they're really good at is creating a nice baseline. They really get you to the beginning of the starting line.

And I'm wondering, given the economic crisis, are more organizations going to be just putting their budgets into getting that check-the-box compliance, or they actually going to be leveraging it, do you feel, to address IT security as a whole?

Because I think for years, we've been saying check-the-box is not enough, I'm just wondering with these economic problems, you know, what's going to happen?

Nick Selby: Well, I mean, it's a really, really, great point. It's one that we actually tried to bring up at PCI, and didn't have much luck in bringing up. You know, the fact is that SOX really was a roar shock test. It was what your auditor thought it was, and what you thought it was. And you sort of, you know, felt your way along. And I think that that was on one end of the spectrum. And on the other end of the spectrum, there's this incredibly descriptive, incredibly prescriptive PCI standard. And, you know, as a baseline, it's really, really great.

As a matter of fact, the thing that we like so much about PCI is that they were telling you to do things that most of us took a look at and said, "Hey, if you're smart, you're probably doing this already. You should be doing all of it."

When you start getting into situations where the rule to which you have to comply, it is so detailed, and so overly prescriptive that you end up having arguments with larger merchants that the rule set is actually stopping them from being secure. They're reducing their effectiveness. We've heard this a lot around malware requirements, you know, anti-malware requirements.

When you've got a rule set that is saying that you absolutely have to have signature based anti-malware.

And your organization might have something that's working a little bit better, the ideas that you have to go back and do this regressive thing for the benefit of the checkbox, as opposed to the ultimate goal of security, it makes you shake your head. It's a very tough line.

And I think PCI is doing a very good job of it so far. But at the end of the day, any rule set is going to be about a compromise between a lot of different people and a lot of different financial interests. And you're going to end up with something that's, you know, the typical camel with nine humps. So, I don't know. I think there's a real danger of that.

As far as the real economic crisis, I'm not sure how much difference it actually makes whether we're in a good economy or a bad economy. I think that you've seen this.

On the vendor side, we're certainly seen it on the analyst side, from talking both to vendors and to end users, that if you tell an organization that in order to do x they have to do y, they're going to do y. And they're probably not going to do z, or seven.

And I think that that's always a problem whenever you're balancing, you know, rule sets against your own posture.

Some of the more enlightened organizations that we see, especially I think that we've seen some real creativity going on in the small market, you know, in the credit unions, and

companies where they just have to be secure or they'll die. You see people actually going off and doing some very, very constructive things.

They meet the compliance requirements, and then they go farther because they're acting proactively, and maybe it will cost them a little more upfront. But they know that they're going to get the savings down the road by, you know, avoiding being that next CNN highlight.

Brian Contos: Based on your experience, I couldn't help but to bring myself to ask you this question. In terms of network security, do you feel it's been completely commoditized at this point? I know a lot of people talk about network security as sort of the plumber's pipe wrench, in terms of how you address it. It's very finite - You know, you've got ports and services. You've got OSs, You've got patches - as opposed to something like application or database security that is really quite infinite, and customized.

It's more like the whole tool set of when you're looking at how to protect from that. Have we really done all we can do in terms of network security have the protection mechanisms? I guess more importantly, have the attack vectors moved beyond network specific attacks in general? And are they becoming more application and database focused in your opinion?

Nick Selby: You know, I'm the world's most incompetent Pen tester. And anyway, I worked at a Pen testing company. And I was the guy who explained what was being done, not the guy who actually did it. So, I'm not going to even try to be the guy who tells you that from personal experience I know, you know, that I can attack more things on the network and the applications. But, I will say this, we've got a lot of antidotal evidence.

And a lot of people who are a lot smarter than me are saying that the real issues are less, I think, around, the positive of targets on the network. And they are the cornucopia of targets in applications.

And I think that it's simply, people are moving to the lowest hanging fruit, and the lowest hanging fruit is elsewhere right now. I think it's a great opportunity over the coming year or so. We said before, there's sale on.

There are a lot of companies that are, you know, great companies with really good technologies and customers, and maybe not good access to credit, maybe not good access to, you know, management who really understands how to kind of manage their cash on the way through this - the economic crisis.

And those companies are going to be going on the block. We've seen it begin. I think that there are a lot of companies out there that are in real dire straits. Everyday that goes by, their situation gets worse. It is going to be a beautiful market for the larger vendors in networking to pick up a lot of great technologies.

And I don't by any means think that that commoditization of things, things like IDS and IPS and certain basic network security stuff, I don't think that commoditization is an indication that it's dealing with something that has been fixed.

You know, there's a billion dollar industry in intrusion prevention, intrusion detection. And those things aren't going away.

I think there are some tremendous opportunities to shore up network security right now as the vendors are able to buy a lot of companies that are going out while the attention is on

applications, and web applications and exploiting those other lower hanging fruits that are outside, that's going to keep people busy for quite a long time.

So, I'm not really sure if commoditization is necessarily a bad thing. I certainly don't think that the problem of network security has been solved. I think that we can always do things better.

I noticed that SSH, you know, the company not the open source project, SSH is making a lot of money this year just doing, you know, straight up conversion of FTP in clear text over to SSH or SFTP. There are a lot of bad practices out there. So, we can always get better.

And I think that actually those bad practices in network security are going to create a lot of opportunities, a lot of buying opportunities.

Brian Contos: As the research continues around these drivers for outlining crime, and how these businesses operate, to see where their attack vectors are focused, if they're purely going after, you know, breaching someone's database and extracting sensitive information either directly or through a web application. Or if it's more wrapped around other types of attacks that are more network centric in order to leverage systems as part of their bot army to conduct malice service attacks, for example, on other organizations.

I think there's going to be a mixed bag. But, that's definitely an interesting point that I'll be looking for.

Nick Selby: You know, one of the other things that I think is really important to know, if you take a look at attacks, you know, card processor attacks, I think it actually speaks to that network security, some real fundamental network security things. I don't think it was about how they got into the network as much as what they did once they were there.

And once they became resident on the network, and the establishment of ad hoc business processes, the establishment of, for example, batch processes that are grabbing large quantities of data and sending them somewhere, these kinds of things are exactly the kinds of activities that you would expect your network security stuff to be looking for and alerting you to.

And I think that the fact that we've got so many breaches done in this way, that we've got so much corporate espionage happening in this way, speaks to the fact that while it might - the technologies might be commoditizing, the problems are still there. And they're very, very, real.

And the need to notice things like where your data is moving, and how your data is moving on what you would might, you know, in a more quaint time might consider inside your network, which brings up overtones of re-perimeterization.

But, you know, even if it's in an environment that you trust, the idea that somebody can create an ad hoc business process, and you not notice it, speaks to a much larger problem of not understanding your own network security.

Brian Contos: Interesting. Nick, I'm sure you're asked this all the time. What's the next, quote/unquote "big thing" in security?

Nick Selby: [laughs] It just happened.

Brian Contos: [laughs] You know it's funny. People ask me this all the time. And I don't know. I wish I knew. But from an analyst perspective, you guys certainly get a lot more exposure out there to being able to answer this question. According to Nick maybe, what's the next big thing?

Nick Selby: And the best part about that is I don't have to be right. I just have to be quotient. [laughs] If I'm right, then I look really smart. And if I'm wrong, people forget.

Brian Contos: That's right.

Nick Selby: You know, I know that - I'm really not even sure what the next big thing is. I know that there is a lot of - I would suggest that the next sort of meaningful big thing is getting clarity around what people are talking about when they say - when they're talking about virtualization security, when they're talking about cloud security. It's great to roll off those terms and say. But what actually are you talking about? There's so much involved there. And there're so many unanswered questions. The scope of those statements is so wildly interpreted.

I think that actually, the next big thing is clarity around what it is that we're trying to secure, moving away from sort of, you know, "Well it's - We're trying to secure the cloud." Well, what exactly does that mean? You know, getting away from the buzz phrase to things that we can understand.

We can break down into components, and see exactly what we're protecting and what we're defending against. And I think that is really the next big thing.

A lot of - I think we're in, because of the economy right now, this is a time of regrouping. This is a time of acquisition of a lot of technologies that might not have made it, or technologies that have been out there and maybe re-purposing them.

It's interesting to see that a lot of the technologies that are being picked up recently in Fire Sales are going to be sucked up into a larger organization that might use a piece of what the start up had been trying to do, but in a completely different way.

So, we think this is kind of an evolutionary process over the next year. But, I think that the next big thing is really coming down to just definitions of what are these big fuzzy terms, cloud, and virtualization? What do they mean to us? How can we take action?

How can we do meaningful things here, and allow these technologies, and these trends to help our business, and help us make money in a secure way?

Brian Contos: Did you have any last comments or thoughts that you'd like to share with the audience before we let you go?

Nick Selby: [laughs] Actually, it's one of the things - I don't really. I've been thinking about some of the companies that we think are in the meantime, are going to do well, over the next say year or so. And some of the things that we've been seeing is companies that are in the business of helping you get more out of what you have, comes down a lot down to configuration, I think, configuration both in the world of basically gateway stuff, firewalls, infrastructure, making sure that those things are working properly.

And configuring machines so that you can tell that things have been changed in a way that might be meaningful.

Cyber Crime, Data Security, SOX, and PCI with Nick Selby

And also, I think, taking a look at products that are able to detect weird things happening, both outside and inside. And that seems like a fairly transparent push towards actually what you guys do. I think that what you guys do is fairly interesting because you're both outside and back end on the database.

I think that there are a lot of forward thinking types of products. And I'm speaking now about both products and services that are looking outside networks, outside traditional perimeters, and trying to be more proactive about spotting threats before they get into, or around, or in proximity to key systems and mission critical systems.

So, we're looking at companies that are offering forward intelligence on for example, targeted malware against certain industries or targeted attacks against certain industries. We think that that's - That's an interesting area that ties into our overall theme this year of taking a look at crime.

And it's a bit more reactive than the kinds of things that we're looking at in terms of how the business models work.

But, it's a lot more proactive than what has been the case which is that you sit there and you wait until you've been attacked and then you do something.

We think that enterprises are much more interested these days in finding out a little bit more, a little bit in advance, what might happen today, what might happen tomorrow, and then, being able to take proactive steps to avoid being hurt by them.

Brian Contos: Well Nick, as always it's a pleasure talking with you.

Nick Selby: Thanks a lot Brian. I appreciate it.

Brian Contos: And hopefully, we can have you on the show sometime again in the future.

Nick Selby: I'd like that a lot.

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.