

PCI War Stories from a QSA – an Interview with Branden Williams – QSA with VeriSign

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 Branden Williams, QSA with VeriSign. He has 14 years of experience in the security and compliance space and is an adjunct professor at the University of Dallas's Graduate School of Management, where he teaches in their NSA Certified Information Assurance program. He is a PCI practice lead with over 80 certified QSAs globally. He has led and delivered security-related assessments for clients in the financial, retail, healthcare, manufacturing, utilities, transportation, service provision, and industrial sectors.

He is a CISSP, a certified information security manager, a qualified security assessor or QSA, and a certified payment-card industry security auditor and manager. He has a Bachelor's of Business Administration and Marketing from the University of Texas in Arlington and a Masters of Business Administration and Supply-chain Management, Market Logistics from the University of Dallas.

Welcome to the show Branden.

Branden Williams: Thanks for having me.

Brian Contos: I guess it wasn't that long ago when we just did our PCI webcast. By the way, anybody that's listening in on this podcast and is interested in getting a little bit more information on PCI and some case studies and a little bit more background on what QSAs do, please go to imperva.com. We did a joint VeriSign-Imperva webcast, and I think it will complement this podcast very well. Branden, before we get started, you work on a number of very interesting projects, literally around the globe, with different industries. What have you been up to lately?

Branden Williams: A lot of what we've been working on lately is helping companies not only improve security from a cost-effective perspective, but also looking at PCI and other compliance initiatives from a maintenance perspective. We learned a couple years ago, after doing these assessments year over year, we'd have repeat customers, and they would do an assessment. They'd finally get to compliance. Maybe it took them a year to get there. We'd go away for nine months, come back, and lo and behold, they have gaps again. And the standard hadn't changed. Nothing else had changed, really, in their environment. They just simply hadn't maintained their compliance.

So we started working with customers on ways to maintain compliance and created an offering around it a couple years ago. We started to mature this offering, and we have some large retailers that have picked it up. And it's really part of the whole management process.

PCI War Stories from a QSA with Branden Williams

And I think, as we see some of the court cases that come out after events of the previous year, we'll see that it ultimately is going to come back down to the merchant or the service provider to maintain and be responsible for their own compliance. They're not going to be able to use a QSA as a liability transfer.

And I also think it's going to have some more scrutiny around QSAs, by the folks that are engaging in them. I think that when you look at a price as the only differentiator, people are starting to figure out that when I have two bids for the same piece of work, one's 100K and one's 10K, we're not really talking apples to apples here.

Brian Contos: I think it was interesting. When we did the webcast the other day, one of the questions that came through -- I'm completely paraphrasing this -- was, essentially, "We get credit card transactions through our website, however we outsource the actual processing and the storage of any information to a third party." And I think you had mentioned, even though that's being done, you still have to address PCI, even though that portion's being outsourced. Is that correct?

Branden Williams: Yeah, it depends on how things are set up. And it's a common business model we're seeing, especially for startups or existing companies that may be starting a new business line, that they don't want to have to deal with this whole PCI headache, so they're completely outsourcing everything. Do they pay more for a transaction? Yeah, they do. But that's really what that compliance cost is. So, there's two ways that we look at this. The first way is, if I'm an organization that is completely outsourced everything, so I've got my website, maybe I own my website, but once I get to that checkout point, I hit the "Click this to checkout." I'm then transferred to a payment processor's website. And I'm not on the original company. I'm not on Joe'sWidgets.com anymore. I'm on BankProcessor.com, whatever it is. And I'm doing all of my credit card information there.

If that's how things are working, then the merchant is probably completely out of scope with PCI, because all the information goes straight to the bank. The bank just does wire transfers back to the merchant. And they really can't even get access to their credit card information at all. If the merchant can get access to the credit card data, then wherever that does happen, that would need to be under review.

And then, in the "worst case scenario" from a scope perspective, if that merchant just uses the API from the processor, as opposed to completely shipping the web traffic over there to try to maintain that whole brand centric thing, "You're going to trust Joe'sWidgets.com. Go ahead and put your credit card number into Joe'sWidgets.com." And then, I send it behind the scenes over to one of these processors. You absolutely still are compliant.

I think one of the misconceptions that a lot of retailers have is that if you don't store data, then you don't have to do any thing with PCI. That's clearly not the case. Store process, transmit, anything, any time that data touches any piece of your network, if it does touch it -- regardless of whether it's stored there or transmitted through -- that's something that a merchant does have to deal with from a PCI compliance perspective.

Brian Contos: Branden, what are the biggest mistakes that organization makes regarding PCI? Maybe it's one. Maybe it's a handful. But, what are the pitfalls that you keep on seeing?

Branden Williams: Well, there's a couple. I mean, if you look at the recent news, I think the biggest mistake is that the organizations are blindly trusting what a QSA might say, or

PCI War Stories from a QSA with Branden Williams

completely pointing to the QSA as, "This is my source. This is my expert. I'm only going to listen to what they say. I'm not going to try to challenge what they say. And in fact, if they say I'm compliant, even though I might know that there's some process over here that's not compliant, I'm not going to say anything because I'm going to treat them like an auditor. I'm just going to get my check mark and then get on with the rest of my life." We've heard that phrase a lot of times from customers where they say, "Boy! I sure will be glad when this PCI thing is done so I can get back to my real job." And that's just an example of another company that just doesn't get it. They don't understand what this means. And they're headed down that road of, "It looks like we're compliant on X date. But four months later we had a breach. Why is that?"

Well, it's because your employees don't care. Or if they care, they're not really baking it into the culture. You don't have top-down support. There's a lot of issues that range from how the culture inside of a company deals with things like security and PCI. And if you don't have good investment, and you don't have good top-down support, it's going to be challenging.

One of the other things we see is that security and compliance tends to be buried inside the IT organization, or even maybe senior inside the IT organization. But regardless, having that function inside of IT, doesn't solve that whole, "I'm trying to make sure I'm compliant and secure problem."

Because IT -- The CIO and the CSO have different jobs. They have different things that motivate them. They have different outcomes for what they are trying to do, so putting them in the same bucket causes problems. And that would be either way, if the CIO reported to the CSO, or the other way around. Those are functionally different areas that need to report separately in the organization.

As far as other big mistakes, I think a lot of it has to do with the maintenance program that we talked about earlier. We did a study a couple of years ago. And one of the things we found is that the top thing that failed, the top requirement customers failed was the scanning requirement. It was the requirement 11.2.

And you kind of sit back and you think about this as a security professional like, "How is this possible? I mean, this is the easiest requirement." I go contract with a stand vendor. They scan my stuff. You know, they're pretty much all the same. I mean there are some variances between them. But they scan my stuff. I get the results. I fix it. And I move on with my life. How is it possible of her not passing this requirement?

And then, we found it was a couple of reasons why. The first reason was that the original inside guy that used to do the internal scannings -- remember, quarterly scans are to be both internal and external, the internal scans that the company can do.

So when the sourcing folks learned about not really a loophole but that stipulation, they'd say, "Well, we're not going to pay somebody to do this. Internally, we'll just do it. And we'll find a guy that's got the tape on his glasses and kind of a geeky guy that sits around, and nobody really knows what he does but he pokes around in computers a lot." He says, "Yeah, I can do it."

That guy is not as relevant in the organization as he used to be. So he has a different job now. He's grown up. Maybe he's leading more of a leadership role. Maybe he's getting into the strategy. Or, quite frankly, maybe the organization moved on and he didn't, and now he's not with the organization anymore. So the internal scans is one that people fail a lot.

PCI War Stories from a QSA with Branden Williams

And then the second piece of that is you have to actually scan until you receive a clean scan. So, if I scan it and there's a vulnerability, I have to fix it and re-scan to show that for that quarter, that 90 days of time, I actually do have a clean scan, and here it is. And that's the two main reasons why people fail that requirement. And it's really just a simple management and administrative process that people forget.

Brian Contos: Now, Branden, when people talk about security and we talk about compliance, you look at the media, it's really easy to get into all the gloom and doom of people just missing the boat and not doing things right. But I think you've got a few examples of, actually, people doing it right and some of the steps they took to be successful.

Branden Williams: OK. The companies that get it right, I think the first thing, when you talk to these companies, if you ever meet someone at a conference and you happen to start talking about PCI, and they just don't seem like, it's like, "Yeah, we struggled to get it moving. But we seem to have a pretty good handle on it now, and it doesn't seem to bother us as much anymore." Usually what those companies have that the other ones don't is they have a process to maintain their compliance, whereby they have management confidence that they're compliant every single day, every hour, every minute, that they know, yes or no, "Am I in compliance or out of compliance?" And if they're not, they usually know exactly why.

For example, "Well, we have this one server. It's giving us a little bit of trouble. We had to wait three days to patch it, so we're technically out of compliance for these three days. We've taken some additional risk mitigation. We put that in play here. So we don't have to worry that this is going to be breached. It's not a critical thing. We do want to fix it. And we're just going to be three days behind. So we've mitigated the risk, but we know that it's still not compliant with PCI."

But once they walk into their assessment, they walk in knowing that they're going to pass. They know. There's no question that when every single interview occurs and all the observations occur that this company knows: "I know the outcome before we even start."

And I think that's the key. For a company that's doing it right, they have a process to maintain it. There's things you have to do throughout the year to maintain your compliance. They take it seriously. They have adequate budget money. I'm not saying that it's a lot, because you can do a lot with a little when it comes to this stuff. But it is important to use a good suite of tools and a good mix of tools and have knowledgeable people working on this stuff.

And one of the analogies that I use is it seems like, in some places, the compliance departments end up full of ex-auditors. And while that's not necessarily a bad thing, what sometimes happens is they don't really understand the security implications or what the standard means.

And so the analogy that I draw is, if you were a company that had your accounting office, you wouldn't just staff that accounting office, from the top down, with people who went to night school to get their CPA degree. Half of them have passed and half of them haven't, but they have accounting degrees. That's not what you're going to do.

You're going to have a few really key people in strategic positions that are experts on this stuff, and then you'll farm some simpler tasks down to the folks that haven't really ascended to that level yet.

PCI War Stories from a QSA with Branden Williams

The compliance department is not going to be nearly as big as many of these finance departments. We're only talking, probably, a few people. But I think that that point still should be valid. From the top down, in your security organization, you have to find people on the top. You have to find people who can speak to executives, and speak to them in a language they can understand, and then also understand what these tech guys are doing and understand the security implications of day-to-day work.

And the selling to management and the business savvy becomes less important as you move down the chain, and it's more important to have that tactical knowledge around security and compliance. And the companies that really get it right, they've built that, whether it's sending people to training or giving the people that wear the multiple hats, giving the compliance hat to the right people. It just takes practice to get it done. And the folks that have taken it seriously, they've succeeded on it.

Brian Contos: It really sounds like it's striking the right level of balance between tactical and strategic initiatives and getting the right level people within each of those to participate and work together. You don't just want the very techie person trying to run the whole show. But at the same time, you can't just have a high-level management person trying to do it all, because there's gaps, of course, in each one of their skill sets.

Branden Williams: Right.

Brian Contos: When we talk about PCI, probably more so than a lot of standards and regulations out there, applications and databases certainly come to mind. How important is security around applications and databases when we're talking about PCI?

Branden Williams: It's very important. In fact, there's certain sections of PCI, namely section six, that really focus on the application security. Of course, your pen test has got to include an application test. And then, also, when you look at requirement 10, for logging, there's a whole lot of stuff in there about databases, that databases would be subject to, right? So, if I've got large data stores that have credit-card numbers in them or transactional records, when I'm accessing that sensitive data, I need to make sure that that stuff is logged. I think that when you look at the applications and database security, one of the things you can do, before you even start kind of looking at all the suite of tools and everything out there, "How do I attack this problem?" You can say, "Well, I don't really necessarily need all of this data."

And if you go through the exercise of purging a lot of the sensitive data, a lot of the data that's covered by PCI, I think that companies will quickly find that, "Hey, maybe this problem's not as big as we thought it was." And once you can make the scope manageable, I think that that allows people to then start taking the first steps to get things done and move to compliance.

From an application security side, when we talked to Visa, the last several times that we've talked to Visa, they have been very interested in talking about application security. The other thing that they talk about a lot now is PIN-debit security as well.

But from the application side, they've seen a massive up-tick in SQL-injection attacks. And these attacks are getting more complex. And because the applications and databases grow in complexity and features to try to capture more market share from customers, the developer base gets bigger, the code base gets bigger, and the likelihood that you're going to have problem also increases.

PCI War Stories from a QSA with Branden Williams

We've worked with customers from all over the globe, where they think that they've got everything set up: "No problem. We're going to be great on this application side." We send some of our guys over there. We do an application test, and lo and behold, very basic things, like cross-site scripting and SQL injection, are ones that come up on almost every single test that we do. And it's usually some ancillary functional that happens, or something behind the scenes that people don't pay attention to, that causes it to happen.

And I think part of the reason why it's not caught on a more ongoing basis, there's kind of a funny thing with how the external scans work for PCI. Granted, if you have an annual penetration test, it should cover this. But the application component of the quarterly scans for PCI don't require you to step past the login screen.

So, when I'm looking at cross-site scripting and SQL injection, I'm really only looking at the login screen itself and, if I have a catalog, I'm looking at the catalog. Anywhere where there's dynamic content on the website, that's basically what I'm limiting my test to.

So, yes, that would be a very telling thing if someone came up with some of these vulnerabilities on those screens. But what we are finding in our experience is that there are a lot more vulnerabilities once you've authenticated as a valid user.

And for almost every single e-commerce site, you don't have to get permission. You just, "What's your email address? What's your name?" and sign up. You don't even have to put payment information in to create an account. So to get a valid account for these applications is relatively easy, and that can open up the application to a whole nother set of vulnerabilities that the folks that are doing the testing may not have paid attention to.

Finally, when we look at application security, there's not enough people doing code reviews. I'm not talking about the peer code review that is required by XX 6.3. I'm talking about someone buying a company or a tool to do the full top-down code review to understand where these vulnerabilities could have been created in the system, where they started. It's understanding that an application security test is only going to find so much. You have to work through the interface.

How do I find the most vulnerabilities? Scanning is going to find a good number of the most common ones. An application PEN test is going to find several more, just based on what you do. But a code review will typically find the most and be the most complete assessment simply because of how it works.

If the tool is good enough, and you're building this thing in the background, running all the tests, and you've got a BCS machine and can do all the steps to do the code review, the result that you will get out of that will be much better than you will get out of the others. Quite frankly, when I'm looking at in from a PCI perspective, I don't think there's many QA who would not accept a full code review in lieu of an annual PEN test.

Also, remember that that's a good zero-impact. Nobody is testing your production systems. They can take your production code and run it offline, and put it in a test environment and see. But that opens up a whole new scenario of tests and when you can do this. I think people would be happy to know, hey, I can run an offline test in November, say November 30 when I'm supposed to have this network free. I can't touch anything, I'm just monitoring stuff, but maybe I can get some consultants in here to do this work behind the scenes so that I'm prepared for my next assessment come May or June.

PCI War Stories from a QSA with Branden Williams

Brian Contos: Yes. I've always been a big fan of just what you said. You want a security assessment and a code review. You want to also run a web application firewall. A lot of people say "Is it either/or?" Just being in security for so long, with the mantra of defensive depth instilled in you, I want to have multiple approaches. Just like you're going to do network vulnerability assessments and networking scanning, and patch those system, you have to apply that same logic. The logic doesn't map up exactly between the data side and the network side, but some of it does. Certainly scanning, code reviews, and firewalling go hand in hand for a strong security posture.

Branden, we have about time for one more question. What do you see as the future for PCI? What should we expect in terms of evolution or changes?

Branden Williams: The thing with changes when it comes to the actual standard itself is that change usually comes on the heels of breach data. As certain types of vulnerabilities become more prevalent, or the attacks are more frequent or more successful, then you will see more requirements around them. It's a little bit behind. Stuff that is in the standard today is still two to three years behind what is actually being attacked out in the field. Now, that does not mean that it is invalid. It means that PCI's great baseline is to bring people up to a minimum, and then you should use security on top of that to better your overall posture. I'll tell you one thing I'd really like to see. I would like to see the forensic process move under the guidelines of the counsel itself. Right now, if there is a breach, the forensic process is handled by the brands and the banks involved. The counsel does not get access to the forensic reports.

So when you look at the Quality Assurance process that the counsel is trying to roll out, there is a piece of it that is very valid. Looking at the deliverables and making sure that they are complete is extremely important to creating consistency inside of our industry.

But the only issue there is that we're only looking at the final work products. We don't have the information that went into creating that deliverable, such as supporting documentation, the interviews, or being on-site and watching the methodology. That stuff doesn't go into this Quality Assurance process. It's because it has to go in stages and they have a limited staff, I understand that.

The Quality Assurance process, as it is today, will be beneficial, but it seems to be missing this closed loop. All right, we've had three breaches now of companies that had believed they were compliant, because the QSA told them they were.

Well, shouldn't the counsel be able to take a little more action and look to say, OK, is there really a challenge with our QSA program? Are our QSAs doing all of the right things and it is really those merchants and service providers that just completely dismantling everything when they leave? OK, well, we can understand that. Our QSAs are doing exactly what they are supposed to do.

Or is it a situation where the QSAs are maybe not doing everything that they need to be doing, or not doing it correctly? Now we have situations where companies, delusion or not, truly believe that they are compliant because of what a QSA told them. Then they end up breached, and during the investigation you find out, wow, you were better than 70% on most of your requirements, but you missed some pretty significant things in your compliance review. You should never have been compliant.

There are discussions like that going on in the news media and the blogosphere. All this stuff is happening, but there's really not a whole lot of actionable things that are happening.

PCI War Stories from a QSA with Branden Williams

The only exception I can think of is that right now there are two QSAs under remediation from the counsel as part of the QA program.

What does that mean? You can look at it and say either that the deliverable that they gave them just aren't completion, or the QA process is pretty hard to go through. I've looked at how they grade rocks. It really does fundamentally change how a QSA needs to prepare it to make sure that it is complete.

So I would love to see that type of change happen. I also think that we're going to see a lot of outsourcing occurring. I think that merchants are going to get fed up with this. I think that they're going to find as many ways as they can to make PCI not apply in their environment, whether it's end to end encryption from the actual PIN entry systems and the acquiring bank, or just by saying "We're not doing any of this stuff anymore. We're going to farm this over to a third party to manage and maintain. We'll just take some wire transfers for this. We're retailers, not payment security professionals. We're paying the professionals. We retail. We're good at selling stuff and getting people to part with their money. That's what we want, exchange for goods and services."

In fact, we had one of our customers that told us that. They hadn't been accepting credit cards that long. After looking at what it was going to take to become compliant, they just said, "I think we're going to just not store any of this stuff post-settlement. Once we settle, we're going to purge it all, and if someone comes back with a chargeback, we're just going to pay it. We're going to ignore the chargeback costs, because it costs so much more money to do this. Because our business is already largely task-based, it's not going to be that big of a deal for us."

I would also be very interested to see if the cell companies could come up with a similar technology here in the US that they have in Asia with SIM-based payments or mobile phone-based payments. That would almost eliminate the card brand market entirely, with the exception of mobile phone companies accepting credit cards in the form of payment. It's just another way, another payment instrument to use since they get savvy to where they don't have this data, don't need this data, or simply outsource big portions of their infrastructure so that they're not responsible for it.

Brian Contos: I say that nobody is in business to be compliant, but it sounds like people are actually changing the way they're doing business because of compliance, which is interesting. It is interesting hearing these people entering or possibly modifying the way they do business because of the regulations. That's fascinating.

Well, Branden, I wanted to thank you so much for joining us on today's podcast.

Branden Williams: Thanks, I appreciate it. I appreciate the time.

Brian Contos: To our listening audience, once again Imperva and VeriSign have a partnership between our two organizations. Recently we did a joint WebEx on this subject. If you go to imperva.com, you can find that. You can hear and see a little more of what Branden has been talking about here. Thanks again, Branden.

Branden Williams: Thank you.

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