The Seven Deadly Sins of a QSA

Whitepaper | February 2011

BrandenWilliams
SECURE BUSINESS GROWTH

Table of contents

Introduction 3

Sin #1: Making Up Requirements 4

Sin #2: Compensating Control Chaos 7

Sin #3: Drunk with Power 11

Sin #4: Buddying Up with an Executive 14

Sin #5: The FNG 17

Sin #6: Q/A Tunnel Vision 21

Sin #7: Bowing to Threats about the Future 23

Final Thoughts 25

People make mistakes. And in a people business like consulting, you can expect to see more than a few of them.

This paper explores seven common mistakes Qualified Security Assessors (QSAs) make. I am speaking from a position of authority because I have made a few of these mistakes during my seven years helping companies comply with PCI DSS (and CISP/SDP before that). At the peak of the PCI remediation boom, I managed a team of over eighty QSAs who made many of these very mistakes. *Mea culpa* sessions are never fun, but the good news is as long as you walk into the meeting with an open mind and a calm temper, you are guaranteed to learn something.

Not all problems are caused by QSAs. Merchants and service providers are just as guilty of making mistakes. You can find any number of articles beating up merchants or service providers for numerous reasons, but the goal of this paper is to illustrate seven common mistakes that QSAs make, and what to do if you spot your QSA making one of them.

Not all problems are caused by QSAs. Merchants and service providers are just as guilty of making mistakes.

Readers of this series will learn to spot some of the most common mistakes, their impact on your organization, how to deal with them if they come up, and how to avoid them all together.

Sin #1
Making Up Requirements

BrandenWrites

One of the most common mistakes QSAs make is to simply make a requirement out of nothing. Don't fool yourself into thinking PCI Assessing is simply black and white judgement calls; PCI DSS is complex. In fact, as a security professional, it's easy to take any good security practice from your brain and tell someone trying to comply with PCI DSS that it needs to be done. For example, changing passwords on a somewhat regular basis is a practice that we all hate doing, but force our users to do anyway. Even without looking at PCI DSS—a standard that has the word "security" in its name—a QSA could tell someone to set up some kind of password rotation scheme without even thinking about how it translates to Requirement 8.5. But what if our QSA is a security professional that believes more rotation is better[1]? He might require a company to expire passwords monthly because he knows that PCI DSS requires rotation, but maybe can't remember exactly how often rotation is required, so for this merchant or service provider it just became monthly.

PCI DSS only requires passwords be expired every ninety days, per Requirement 8.5.9—clearly less frequent than what this QSA just required.

While this example is a relatively basic one, you can imagine that this happens often when there are now thousands of QSAs globally and they have 250+ requirements to draw from at any given time. So how does this happen?

Mis-hearing the Trainer

QSAs must pass an evaluation from the Council every year in addition to earning at least forty CPEs in order to maintain their QSA designation. Prior to 2010, this meant finding a QSA Requal class near you and having your primary contact book your attendance in said class[2]. Trainers come and go as we have seen over the years, and I sat through a session with a good number of my team lead by a new trainer a few years ago.

One of the most important steps a QSA must get right is choosing the correct scope for the assessment. Getting that step wrong sets the whole assessment and the PCI experience up for failure. This topic tends to be one of the first things that trainers review during their sessions. The theme for that particular year was the introduction of tools that can help a QSA perform assessments.

A data discovery tool that can help someone validate scope can search files for regulated data—in this case, cardholder data. The trainer showed us a free tool called Spider from Cornell[3] lauded as a fantastic asset for any QSA performing an assessment. While learning about how useful this tool could be during an assessment, one of the QSAs on my team took this demo to mean that these types of tools are REQUIRED to comply with PCI DSS. After attending this training he went to a client site and told a customer that in order to pass their assessment this year, they had to install some kind of Data Loss Prevention (DLP) technology, which may include something like Spider. There was no requirement to use DLP in PCI DSS, yet a trained and certified QSA just told a customer they needed this in order to pass!

Assessing against PCI DSS is a learned art that you can only refine by doing many assessments. Two days of class time and a test won't get you that knowledge—a problem

FOOTNOTES

[1] *Hint: more rotation is probably not better.*
[2] *You can now do your requalification online.*
[3] *http://www2.cit.cornell.edu/security/tools/*

we will touch on later. The finesse of a good assessor will far outweigh the technical knowledge of a newbie.

Being a Security Professional

Being a security professional can be a curse when logically thinking your way through compliance initiatives. No compliance initiative should be a substitute for a sound information security program, but we as security professionals often get caught in the compliance trap. We've been beating the security drum for years, yet our musical stylings have gone unappreciated. Enter a compliance initiative and all of the sudden someone is forcing the business to do what we've been telling them to do all along! We tend to take advantage of this new security spending windfall and add all kinds of stuff to purchase orders in the name of compliance.

QSAs are guilty of this as well. Often times a QSA knows there is a security issue that needs correcting and tells a merchant to do something to satisfy it in the name of PCI DSS. For example, the process of scanning a location quarterly for rogue wireless devices is a badly constructed joke whereby the punchline is met with crickets from the crowd. If you are serious about detecting rogue wireless devices, you need to have something constantly searching and cataloging, and you need personnel to walk the floors to look for things physically out of place[4].

No compliance initiative should be a substitute for a sound information security program, but we as security professionals often get caught in the compliance trap.

So if you approach PCI DSS from a security professional's point of view, you might make up a requirement for Wireless Intrusion Detection Systems (WIDS) to be installed as a means to meet PCI Requirement 11.1. In fact, I was guilty of doing this for merchants using WiFi point-of-sale (POS) devices. I recommended this to one of my customers even though there is nowhere in the PCI DSS that supports this notion. It's darn good sense, but not a requirement.

How to Avoid a Made Up Requirement

The only way to avoid a made up requirement is to ensure that there is material in the PCI DSS that supports a recommendation before a it's made. There are two main areas where you can find information on how to handle strange situations—PCI DSS itself as well as the FAQ that can be found on the PCI Security Standards Council's website. The "Navigating PCI DSS" series is also useful, but supplementary and cannot be assessed against. Any guidance taken from documents other than the PCI DSS should be written up as a compensating control where appropriate.

Additional documentation such as Special Interest Group (SIG) whitepapers, do not indicate changes in the standard and must only be used for educational purposes. For example, a whitepaper from the Virtualization SIG condemning "Mixed-Mode" in large virtual infrastructures may be an indication of what a subset of stakeholders believe, but QSAs cannot act on the information contained within the paper until it ends up in the PCI DSS or as part of some other formal communication from the Council directing QSAs on how to assess these environments.

FOOTNOTES

[4] Also, would the WIDS vendors please stop cheering after reading this. We get it, and we heard you. Every year since this thing got started. And at every community meeting. Go sell your product on VALUE and don't fall into the compliance trap.

Sin #2
Compensating Control Chaos

BrandenWrites

Compensating controls are a challenging and somewhat confusing nuance to PCI DSS. In Chapter 12 of PCI Compliance: Understand and Implement Effective PCI Compliance I delve into this perceived "Get out of jail free" card. Many companies have found this a useful guide for creating compensating controls during their PCI DSS journey[5].

Compensating controls are designed to allow companies to meet the controls laid out in PCI DSS in alternate ways. For example, a company that cannot put Secure SHell (SSH) on all of their routers due to technical constraints and switches may be able to do something different that would meet requirements for a compensating control as laid out in the PCI DSS Glossary:

> Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints … Compensating controls must:
>
> (1) Meet the intent and rigor of the original PCI DSS requirement;
>
> (2) Provide a similar level of defense as the original PCI DSS requirement;
>
> (3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
>
> (4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.[6]

Before any control could be considered for this perceived loophole[7], it must comply with all of the above restrictions. In my experience, "security-deferring" compensating controls tend to be more costly and troublesome to an infrastructure long-term than just fixing the problem. I've seen some ridiculous controls proposed, erring on both extremely conservative and extremely liberal interpretations of the "intent and rigor of the original" control. Let's walk through some of the issues we might find.

"Security-deferring" compensating controls tend to be more costly and troublesome to an infrastructure long-term than just fixing the problem.

The Liberal Assessee

If you are tasked with helping a company comply with PCI DSS without all the resources you need to do the job appropriately, you may end up taking a more liberal interpretation of the standard as a shortcut to compliance. Let me be frank: the only shortcut to compliance is to completely outsource your payment processing environment to someone else. It will cost you more money to process transactions, but that delta in transactional cost over a year might be close to what you should spend on PCI Compliance anyway[8].

Assessees become stage actors at this point in the conversation. I've seen some fairly silly controls argued with Oscar worthy passion. One particular example was a customer of mine that tried to convince me that the basic functionality of Redundant Array of Independent Disks (RAID) is a perfect compensating control for Requirement 3.4, protecting stored data. She argued that any single disk removed from a RAID-5 array would only contain fragments of data and would not yield any useful data to an attacker. While in some cases, she is correct, Requirement 3.4 is not trying to protect the physical security of cardholder

FOOTNOTES

[5] This chapter is freely available at our book's website, http://www.pcicompliancebook.info/.

[6] Quoted from the PCI DSS Glossary, found here: https://www.pcisecuritystandards.org/documents/pci_glossary_v20.pdf.

[7] The rigor by which this standard must be met causes this to be less of a loophole, and more of a quagmire.

[8] For more hot sports opinions on how we ended up in this situation, read this blog post: https://www.brandenwilliams.com/blog/2009/09/08/blame-mbas-for-pci-remediation-costs/.

data stored on a disk—Requirement 9 is. Let's run this through the four tests from above and see what we come out with:

1) RAID-5 as an algorithm does not meet the original intent and rigor of Requirement 3.4, mainly because there are no data protection mechanisms employed either via strong access controls or strong encryption.
2) While this might provide a similar level of defense in the case of physical theft, it's not equivalent. We'd be pushing our luck to call it similar.
3) This is most definitely not above and beyond the other PCI requirements.
4) Finally, RAID-5 as a data protection mechanism is not commensurate with the additional risk of not protecting the cardholder data.

One out of four is not good, and definitely does not meet the litmus test required to consider this a compensating control.

The Conservative Assessor

Assessors are just as guilty as assessees, but lean to the other extreme—especially when they do not understand the technology that enables an environment to function. This is increasingly common as the QSA community gets younger.

Let's say that an assessor does not fully understand networking technologies like 802.1q VLAN tagging and is presented with a problem that requires the creation of a separate management network to comply with PCI DSS. Let's say the control being presented is a variation of our Telnet/SSH example from above. An assessor that does not understand how 802.1q works may suggest that in order to create this management network, each machine must have two dedicated network interface cards (NICs) that go to different physical switches. Now, if the targeted switching network can only be administered via Telnet, I might agree depending on the architecture of the network and how far the trunks go. But if the switching network isn't the issue (maybe it's a group of legacy routers), 802.1q might be perfectly acceptable with the proper configuration and controls.

Assessors are under tremendous pressure to get the full PCI DSS picture at a company in increasingly shorter amounts of time. Along with that, the PCI Security Standards Council requires any QSA to sign up for uncapped indemnity. That very clause has kept the Big Four out of QSA work, and recently other very large firms that see the risk as too great. Because of this, you can expect that inexperienced assessors are going to lean far to the conservative side.

The Role of the Acquirer

Ultimately it is the Acquiring institution that must approve the compensating control. If you are like most companies, you most likely are dealing with more than one Acquiring institution, so remember, any control you propose should be approved by ALL of them before proceeding. Imagine the difficulty of getting your Visa/MasterCard acquirer to agree with American Express, and then Discover! It's hard enough to get one institution to agree, but three? Consider this before you bet the farm on a flimsy compensating control that doesn't solve the underlying problem.

How to Avoid Compensating Control Chaos

There is really only one way to avoid getting into a tug-of-war on compensating controls—don't use them. Unfortunately, for most companies, that is virtually impossible. For

those of you that must use at least one compensating control, be sure to document them thoroughly, and plan on over achieving just a bit to show the assessor you are not just trying to scrape by. If you have a long-term remediation plan to address the root cause of the issue, disclose it with milestones and owners. This alone will go a long way to showing both the assessor and the Acquirer that you have thought your way through your design of the control, and have an exit strategy planned. Compensating controls must be written up with each Report on Compliance (ROC), so expect a savvy Acquirer to review it each year to see if you are sticking with your commitments.

Sin #3
Drunk With Power

BrandenWrites

QSAs are often in a position of perceived power. They sometimes exhibit authoritarian behavior, often times enabled by the very people they are assessing.

QSAs are just people.

You are hiring them to evaluate your performance against a detailed set of requirements. They are not peace officers, and they are most definitely not auditors[9]. Smart companies will use this knowledge to their advantage and work the psychology of the situation.

The Psychology of the Situation

The QSA is acting in a position of authority based on his role in the assessment process, passing the QSA training class, and his education and experience. Individuals inside companies being assessed rarely know or remember how the world operates outside their organization and struggle when describing how their own company handles PCI DSS. Don't get me wrong, assessees typically know their specific view and scope of control, but they suffer from tunnel vision and often end up living in a compliance silo. Consultants on-site—the face of the company hired to determine PCI DSS compliance—can personify this role of perceived power and authority. Add to that cultural differences (both corporate and tribal) that will invariably exist between these two groups and you can see how complex the psychology of a PCI Assessment can get.

You might recognize you have one of these career authoritarians when you hear him say things like, "I'm going to fail you."

Given these inputs, some QSAs will exhibit some of the worst kind of behavior—the Bad Cop. To paint this picture more clearly, think back to your secondary education around the time you started driving. Do you remember that guy (or gal, no sexism here as I've seen both) that was the career authoritarian? He didn't play sports, he was the referee. He didn't try out for talent shows, he was the judge. He didn't try to make a bathroom pass last all period, he was the hall monitor. He had aviator sunglasses and started growing a mustache the minute he was able. You used to look at him and think, "If that guy ever becomes a police officer in this town, I'm never coming back!" He'd be the guy that would give you a ticket for two miles-per-hour over the speed limit on a deserted street[10]. Career authoritarians seek out jobs that feed their ego, and a few of them are QSAs.

You might recognize you have one of these career authoritarians when you hear him say things like, "I'm going to fail you," or "I can't find my way to pass you on this requirement." Don't be alarmed, just change the way you handle him.

How to Deal with a Power-Drunk QSA

Above all, remember that he's just a guy. He's trying to do his job, just like you are trying to do yours. If you allow the situation to heat up, everyone will suffer. Play the game, work with the guy a little bit. Listen to what he has to say. Ask for suggestions on how you might meet the requirement in his eyes[11]. Overall, he's probably not a bad guy. Maybe he's having a bad day and taking it out on you in an unprofessional manner, but that's a bump in the road that can be overlooked.

FOOTNOTES

[9] Although some may be CPAs.

[10] Don't get me wrong, I have both family and friends that are peace officers and love their jobs. Most officers are not like this guy, but this guy tends to crave positions of authority and could end up in some kind of enforcement role.

[11] You may have to enable him further to diffuse the situation.

The first step is to remember the "No Asshole Rule."[12] Your negative behavior will be amplified and mirrored back at you, most likely escalating the situation out of control. Do the right thing to avoid conflict. If you know that something does not comply with PCI, don't argue for the sake of arguing. Accept that you need to do some work and gather information on how to tackle the problem. Don't let your boss play the "push back and see what happens" card.

If you have clearly met the burden of compliance, don't be afraid to stand up in a calm way. Have a well thought out, well documented argument before engaging the QSA in the discussion.

If you are not getting anywhere with the QSA in this situation, escalate to his manager. Going over someone's head is a very delicate process, and there are only a few ways to get it right while there are hundreds of ways to get it wrong. If you are just playing the odds, this escalation will not go over well. You really need to get your house in order before escalating. If things are still not working well, replace the teams on both sides of the table. Get a fresh project manager on your side, and ask for a new QSA team on their side. Doing so will probably slow things down, put project timelines in jeopardy, and potentially add more cost to the engagement but may be required to have a successful assessment.

FOOTNOTES

[12] *https://secure.wikimedia.org/wikipedia/en/wiki/The_No_Asshole_Rule*

Sin #4
Buddying Up with an Executive

BrandenWrites

Consulting is a people business. People buy knowledge, skills, and services delivered by other people. Unlike a product business, you can't guarantee that each unit is exactly the same, even from the same person. And also unlike a product business, the consultant interfaces on a human level with various members of the executive staff. Strange things can happen when QSAs buddy up with executives. Let's explore a situation near and dear to me.

My Standard > PCI DSS

Executives act different after someone suspects a security breach has happened on their watch. All of the sudden, they get religious and grow a tiny, beating security heart inside their otherwise empty chest. This is, of course, a very broad and unfair generalization as more and more executives are paying attention to information security. My story comes from an experience from several years ago.

A company called upon my group to help them understand if they suffered a breach after they were fingered as the likely common point of purchase. This particular company didn't ignore information security, but they never took PCI very seriously and only focused on some elements of the larger suggested baseline from ISO 17799 (current at that time). Once they were suspected to be the cause of a breach, the information security office was instantly promoted to an executive level and the buzz from the top down was all about being the most secure company in their space. I was pulled aside early in the process and given a specific directive: "PCI DSS isn't good enough for us, and we want to exceed in the following areas." I was instructed to not mark someone's area compliant to PCI DSS in areas where management's standard was more stringent. I was building a good relationship with this particular executive which was paying dividends for my own career.

I had several meetings during that year where managers would ask me to point out exactly where the standard told them to use 256-bit keys instead of 128-bit keys (one of the many enhancements against which I was instructed to validate), and I could only tell them that my instructions from the company were to highlight their name in my weekly status reports until they implemented 256-bit keys. It was a horrible position to be in, because the assessor AND security professional in me recognized that 128-bits of encryption would be just fine.

How to Avoid the Buddied-Up QSA

If you are lucky enough to have one, it's hard to avoid his impact. It could get even worse if the guy is also drunk with his executive-sponsored power. When I was a buddied-up QSA, I told those managers to get a meeting together with the executive and discuss the technical and business constraints they faced. I also instructed them to make sure they do their homework. Don't whine, and don't focus on why you shouldn't meet her standard. Bring everything to the table that is required to meet the executive's directive. This should include any capital expenditures such as hardware, software, and costs of people time, as well as soft costs like lost productivity, other projects pushing completion dates out, and downtime associated with wide scale rollouts (there will be some, no matter how hard you try to avoid it). Most importantly, bring two to three alternatives with associated costs that would meet the base requirements of PCI DSS, and include some kind of roadmap to get your area to the executive's standard. You don't want anyone to lose face here (mostly the executive), and if you can reasonably show a way to get your area to his standard, it will eventually make you a hero (things may be tough in the short term, but think long term).

This is where a good knowledge of business tools like MS Excel will pay off. If you have not learned how to use modeling or Solver inside of Excel, do yourself a favor and invest some time learning this powerful tool. Not only will you make your life easier by allowing the software to crunch the numbers for you, but you will be presenting information back to executives in a familiar manner. Your CIO isn't going to give a rip about the challenges of upgrading a Cisco infrastructure that was not designed for the future or why your life will be painful. It's your job to do these things. But if you present a business argument with a logically thought out solution, you may be surprised at how you get what you need in order to do your job. My final piece of advice: executives tend to have excellent bullshit alarms. Be sure to back up every single assumption and every piece of data used in your model with raw data. Avoid relying on an analyst projection without knowing how they got to that projection. Prepare for an inquisition and you will come across as more confident and more capable of doing your job.

Executives tend to have excellent BS alarms. Be sure to back up every single assumption and every piece of data used in your model with raw data.

Sin #5
The FNG

BrandenWrites

The Flipping New Guy (FNG) causes havoc wherever he goes. He also goes by the Pimply-Faced Youth (PFY) in some circles, and is often labeled as having the talent to tame a lion, but the experience to raise a hamster. He's the guy that just went to new QSA training, passed his test, and showed up to do some good, old-fashioned assessing!

Three Days of Ground School

One summer, well after I became a QSA, I earned my private pilot certificate. If you ask my wife, she will tell you she remembers me babbling all of these fantastic[13] bits of knowledge that I was learning every day, and passing the time in the evening with at least one book in my lap instead of talking to her. I worked hard to earn my certificate, and learn something new almost every time I fly.

Let's say that you decide you want to become a pilot. You sign up for a crash course (pardon the phrase) in flying which includes three days of intense ground school training. Now imagine that at the end of those three days, your instructor throws a set of keys at you and says, "Nice work today! Here are the keys to a Cessna 172. It's full of gas, and the runway is over there. Have fun!"

Terrifying.

Almost as terrifying as a new QSA running his first PCI assessment.

My experience as a QSA is similar to that example in many ways. I took two days of training and passed a test to prove I had retained the information[14]. Just like a student taking a plane up solo for the first time, my first real PCI assessment was frightening.

The only thing on my side during that assessment (other than my training) was the baseline of security and technology knowledge I earned before I started working with PCI DSS. I was an expert at *NIX operating systems, web-application development and databases, and had a good working knowledge of electronic payment processing. But that didn't qualify me to review z/OS systems for compliance with PCI DSS! It took time to earn the knowledge that I rely on now when I am asked complex PCI DSS questions.

Newly minted QSAs rarely have the base of knowledge required to correctly perform a PCI Assessment on their own.

Newly minted QSAs rarely have the base of knowledge required to correctly perform a PCI Assessment on their own.

Identifying the FNG

The consulting business is full of slick salesmen. Were you promised an experienced QSA during the sales cycle? How do you know if they sent a newbie that is good at taking tests? Before you sign the papers on that contract, you should be interviewing the lead QSA that will be responsible for your assessment. Do your research and ask him hard questions. You will be spending some time with this individual over the next several weeks, so you should invest some time to choose a suitable one. Next ask what their team will look like. Some companies will send one lead QSA with a few non-QSAs perform these assessments. You can imagine the issues that will cause down the road.

FOOTNOTES

[13] *My word, not hers.*

[14] *Or could quickly look it up during the open book test.*

The Council provides you with a way to see if the consultants are current[15]. New QSAs will have anywhere from nine to eleven months left on their certification. You won't be able to tell if they have been certified more than once, but you can certainly ask the question of the QSA when she arrives. When it comes to PCI, "Trust, but Verify" should be the guiding principal on both sides of the assessment process.

If you didn't get to do this during the buying process, there are other clues you can use to see if you are dealing with a newbie. Not only will they make many of the mistakes I've identified (and frequently), but they will struggle to get through their part of the assessment. Look for someone with a printed out copy of the standard furiously flipping pages during interviews. No paper? Look for someone staring maniacally at their laptop doing a lot of scrolling. Most experienced QSAs can spout off requirement numbers from memory or have a predictable style they use during the interview process and only use paper or digital material as a reference.

Good PCI DSS, Bad Infosec Foundation

You may also find that QSAs do not understand your environment thoroughly enough to make an accurate compliance call. More executives are telling me their recent QSAs struggle when assessing complex technology implementations.

QSA work isn't sexy like it used to be. Back in the day, my favorite projects involved helping companies rebuild their network to include security to close PCI DSS gaps. I solved complex problems involving hundreds of people, thousands of machines, and millions of dollars. It was taxing on my brain, but I absolutely loved the challenge!

Solving PCI problems five years ago required considerable knowledge of how business processes and technology fit together. Most companies facing PCI DSS today are not first timers. As the saying goes, "This ain't their first rodeo." The crop of folks that solved those PCI problems has moved on to other big issues like healthcare information security, cloud, or mobile computing. The new crop of QSAs is at a tremendous disadvantage because they have significant pressure to deliver engagements in less time. QSAs don't have time to learn about what virtualization actually entails—for example—they look to the Council to tell them what to do about virtualization. This puts more pressure on the company being assessed to get things right instead of allowing QSAs the time they need to really do the thorough job that I personally think needs to be done.

Your QSA may never have administered a server or configured a firewall or managed a Wide Area Network (WAN) or developed applications. This is a different kind of FNG problem than the newly minted QSA as you could have a QSA with a year's experience under his belt, but no real working knowledge of the technologies he is assessing in your environment. This is why vetting your QSA up front is so vitally important to a good assessment and good assessment experience.

Combating the FNG Curse

I may sound like your parents when I say "you will get out of this experience what you put into it."

FOOTNOTES

[15] *https://www.pcisecuritystandards.org/approved_companies_providers/verify_qsa_employee.php*

The easiest way to deal with the FNG is to be prepared! If you have done a pre-assessment and organized your entire project from start to finish, you can guide your QSA through the assessment process in a way that ensures you don't waste your time, and the QSA gets what he needs in order to complete the assessment. You cannot rely on the QSA for everything; you have to invest your own time to fully understand your environment and how payment cards are handled throughout your entire organization. Doing this will make you an MVP at your company as there are probably few (if any) co-workers that can articulate data and process flows, much less call themselves experts in the environment. Like the Boy Scouts of America, be prepared. If you are, this sin will not be a factor.

Sin #6
Q/A Tunnel Vision

BrandenWrites

The Quality Assurance (Q/A) program is in full swing at the PCI Security Standards Council. After companies started taking PCI DSS seriously and retaining QSAs, merchants and service providers realized that not every QSA interpreted requirements the same. One of the biggest complaints about the QSA community is variance in interpretation on key items that could impact the cost of compliance—positive or negative. The Q/A program was announced at the 2008 PCI Community Meeting[16] and began to take effect shortly thereafter. QSAs were put on the remediation list as early as 2009.

Myopic Assessment Views

The objective of the Q/A program was to decrease the variance in interpretation among QSAs and increase the overall quality of assessments. Each QSA company must submit redacted Reports on Compliance (ROCs) from a given time period, and each report is reviewed and scored on upwards of 700 different items.

The results so far? Inconclusive as far as I am concerned. The overall quality of the deliverable coming out of a PCI assessment is improving in direct relationship to this program, but what is missing is that on-site touch and feel that simply is not possible today. The Q/A process has effectively trained QSAs to produce better reports—potentially by pre-writing deliverables before the engagement starts. A solid deliverable is great, but if it does not accurately represent the environment to which is it written, it does no good to the company, their acquirer, and ultimately the QSA community.

The Q/A process has effectively trained QSAs to produce better reports—potentially by pre-writing deliverables before the engagement starts.

One move by the Council that may help close this gap is the institution of the PCI Forensic Investigator (PFI) program, which replaced the Qualified Incident Response Assessor (QIRA) program from Visa, Inc. If the Council can see the forensic report from a breach in conjunction with the original ROC, it's easier for them to take action against a QSA after a breach.

If a QSA becomes hyper-focused on the Q/A program, they will neglect to focus on the real issue—performing a thorough assessment and making sure the deliverable matches the assessed environment. I've seen QSAs armed with "known passable responses" to questions in massive spreadsheets ready to cut and paste away. If those chunks are edited to the environment, there is absolutely nothing wrong with this approach. Lawyers do it all the time[17]. But if pre-written comments are placed in the report without editing, you end up with a document that passes the Q/A process but fails the assessed entity.

How to Avoid Quality Myopia

The only way you can avoid this problem is to watch your QSA operate during the assessment and do your homework on what an assessment really takes before signing a contract. You can obtain the latter by becoming an Internal Security Assessor (ISA) which gives you the same training a QSA gets with a test at the end. Scoping is a big part of the QSA and ISA training, and this knowledge will help you budget for your next assessment. If your bid solicitation process produces quotes with a standard deviation greater than the value of one of the bids, someone doesn't understand your requirements.

FOOTNOTES

[16] *If you are a stakeholder in PCI DSS and are not going to these meetings, you are missing out.*

[17] *In fact, I've wondered if the measure of a good contract lawyer is one that knows WHICH contract to plagiarize.*

Sin #7
Bowing to Threats about the Future

BrandenWrites

Remember when we discussed consulting being a people business? The last sin we will cover is actually one that can be committed by either party. Maybe more accurately, committed by the QSA, but enabled by the assessee. QSAs sometimes give in to someone who says, "If you don't mark this as compliant, I am giving my business to someone else." I'm not talking about a contract issue or some other incidental dispute during the assessment, I'm referring to the rigor of the assessor being used as a bargaining chip.

It's My Way or the Highway

As an assessor, I've been threatened like this multiple times over my career. Having someone in middle management with an agenda (or even an executive) tell you that you need to "change a report because you will be responsible for losing him as a client" is never pleasant. QSAs that bow to this are making a fatal mistake that could cost their customer and employer dearly. Sloppy assessing could lead to a breach and a false sense of security by the assessee's board. QSAs should take these threats seriously, but they should not immediately bow to the pressure unless they realize they made a mistake. If an executive is telling them that two passwords is "basically the same as two-factor authentication," QSAs should stand their ground and calmly explain that the intent of the standard is to actually have multiple factors of authentication, not multiple instances of one factor of authentication.

How to Avoid the Threat of the Future

There is not a cut and dry method for avoiding this one as it tends to be a behavioral response the assessee's organization. Like salivation after hearing a bell, employees panic when they think they might be responsible for their company losing money. If a QSA is not savvy enough to realize how to resolve the situation on his own, this mistake might be the one that does your company in.

QSAs in this situation need to validate their assumptions and be sure they are reading the situation according to the intent of the standard. There is plenty of material out there that QSAs can use to do this, but experience is going to be a big asset. If the QSA is wrong, he needs to adjust his position immediately. If the executive is wrong, the QSA needs to make sure his management understands this may not be the kind of customer they want to service long-term.

In some cases, corporate culture allows or even promotes this behavior. It may be OK in some areas of the business, but it is most certainly not in this one. Companies that discover an employee exhibiting this behavior should take swift action against the employee to minimize the negative effect that one bad apple can have on the company.

Final Thoughts

BrandenWrites

QSAs are human, and humans make mistakes. Over the last several pages we have discussed seven deadly sins committed by QSAs, shown examples of what those mistakes look like, and given you guidance for how to avoid them or navigate your way through them if you find yourself in the middle of one. If you must comply with PCI DSS, one of the best investments you can make in your people is to put them through the same training QSAs go through and have them certified as Internal Security Assessors (ISAs). This way, you will have an additional check to know if a QSA is making one of these (or other) mistakes and have a chance at catching them before they derail the entire PCI DSS assessment process.

Though not all problems are caused by QSAs (merchants and service providers are just as guilty of making mistakes), hopefully the tips presented here will benefit you in your quest to become PCI compliant and your charge to maintain PCI compliance.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH