Herding Cats:
Embrace the ISA Program

August 2010

BrandenWilliams
SECURE BUSINESS GROWTH

In May, I wrote a quick opinion piece in my blog about the PCI Security Standards Council's new Internal Security Assessor (ISA) program. Aside from my fun encounter with the Hoffacino[1], it has been the most looked at post on my blog over the last two months. Why all the attention? I believe that merchants are starting to realize the amount of money they are pouring into compliance and thinking there must be a better way.

Pending the release of the program, I spoke to a few QSAs who were afraid the new program may contribute to a decline in their business[2]. The overall attitude toward the QSA community from merchants and service providers is as poor as it has ever been. I heard from several attendees to a recent Electronic Transactions Association (ETA) event who said the negativity was palpable.

There are a couple of reasons for this, and the blame (or opportunity for improvement) lies in both the assessor and assessee camps:

> 1) QSAs are being held accountable to their work through the Quality Assurance program which ultimately drives the cost of assessments up and starts to level the playing field from a pricing perspective. I understand the average assessment cost is increasing dramatically, and there seems to be a narrowing range of bid prices.
>
> 2) Merchants realize that they can no longer look to a QSA to tell them where all of their problems are, and must actually take some ownership in the solution. In the words of one of my new favorite speakers, merchants and service providers must participate in their own rescue[3].

Merchants that send their employees through the ISA program will ultimately benefit from this investment as they can better hold themselves accountable to PCI DSS. In fact, as a Level 1 or 2 merchant[4], you cannot self assess without sending your employees through the ISA program and having them pass the certification test. But even if merchants don't intend to self assess (and quite frankly, the vast majority should rely on a third party to validate their compliance), the ISA program will still prove beneficial.

If you are a QSA, don't view ISAs as competition. See them as your champion. ISAs are GOOD for QSAs, and as a QSA you should prefer to assess companies that have installed them on their teams. I was speaking to a colleague late last year at a PCI gathering and he mentioned that his last internal PCI assessment consumed over 3,000 hours.

Three thousand hours, folks.

This was not a giant company, though they are a Level 1 merchant. Doing some quick math using standard consulting rates, the price tag for such an effort could be anywhere from USD$600K-$750K. I've seen and performed assessments that big and bigger, but they are usually multi-nationals with many business lines and some degree of autonomy outside their central IT organization. Knowing what I know about my colleague's company, I would have probably scoped the same assessment somewhere between 400 and 500 hours.

FOOTNOTES

[1] *http://j.mp/9EYCeI*

[2] *Though, in essence, overall market pressures will do more to cause that decline than the ISA program will.*

[3] *Thank YOU John Kaplan!*

[4] *Check my blog for details on dates. Yes you can self-assess as a Level 1 merchant, you have always had that option.*

This particular organization will send several people to become ISAs, and will probably continue to do their own assessments, but that is not the norm. I believe companies will invest in their employees to add one or two ISAs to their staff, and use that as a checkpoint to keep their QSA honest, truly understand what needs to be done to comply, and push their QSA to do a thorough job which is not uniformly occurring today.

Companies hire CPAs and attorneys as employees to leverage their expertise, but they still use external accounting and law firms for expertise and validation when they need it. Sure, some PCI related tasks will be taken off the table if companies send employees through the ISA program, but the ones that remain will be considered strategic and be significant for the company providing services on the opportunities.

The future of payment security is certainly evolving, potentially ahead of other data security initiatives. I've lived PCI for a long time, and believe that the problem is now be dramatically reduced. PCI is not the scariest thing out there (by far), but gaining a champion inside the assessed company has potential to create a better end result for all.

Contact information for requests for permission to reproduce or distribute materials available through this course are listed below.

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/.