Herding Cats:
Brave Old World

December 2010

BrandenWilliams
SECURE BUSINESS GROWTH

For those of you that read this column regularly, you know that I typically tie the content contained here into the theme of the issue. I'm breaking away from that trend today, but only to use it as a way to illustrate the need to challenge the status quo.

In the last month we've seen quite a bit of buzz around the new version of PCI DSS. As of this writing, not only has the global standard been released, but the Self-Assessment Questionnaires are now available. Most people that I talk to often use colorful metaphors to describe their experiences with PCI DSS. As a recovering QSA, I find it hard to disagree with much of what they say. Though I take exception with open hatred toward PCI DSS because if companies had not been stubborn about security in the first place, we may not even need PCI DSS.

That's right, I wrote it. PCI DSS advanced information security initiatives more than any other compelling event in the last ten years. For that, we should be happy, even if it means we had to find ways to tie our needs to PCI DSS to get them funded[1]. The somewhat comical part of this whole process is that people spending on PCI DSS compliance did it completely tactically and didn't actually think about the larger information risk management picture, of which PCI DSS is a **sub component**. We did a bad job at helping the business correct their myopic information security posture, and instead used PCI DSS as the stick to get basic security tools and processes in place.

Only now are companies starting to realize that they created an unsustainable auditing cycle that is gobbling up precious resources at an alarming rate.

Back to bucking the trend of topical writing: why isn't anyone at the top asking "why?" Why are we doing business this way? Why did we make these decisions a decade or two ago? Why are these issues a problem **now**, and were the problems present back then?

Maybe these problems did exist, but nobody[2] payed attention to PCI DSS until fines began trickling down in late 2007 to early 2008. Now the pain was real, and it became scramble and crunch time while the economy was circling the drain.

Information is undoubtably valuable, be it to a corporation, individual, or criminal. Yet, we don't really treat it as a valuable asset, do we? Think about how we treat cash. Safes, vaults, armored cars, multiple checks and balances, and limited on-hand supplies help us reduce the risk of cash disappearing. So why don't we do that with information? How do we assign a dollar amount to that value in a manner agreed upon by the masses so we can make our point?

Imagine for a moment, that a retailer stopped thinking about how to fix their legacy systems so they can comply with PCI DSS, and instead thought about how to devalue or remove the information all together. Why should the retailer be the official data custodian of a credit card? They shouldn't, and they don't have to be. Instead of maintaining the data, why not look to another "owner of record" whereby the small amount of data that might be required on a daily basis could be safely obtained? Greater than 99% of a merchant's transactions are good, so why do we need to increase our risk 100-fold because of a meager fraction of 1% of our volume that might go sideways on us?

FOOTNOTES

[1] By the way, it's NOT cool to draft up a $16 million, out-of-cycle request for funds and then say, BRANDEN SAID I HAD TO DO IT! Yes, that happened. You know who you are.

[2] That's an unfair generalization, but when you consider 7-8 million merchants in the US, it's a safe one.

We have to get smarter about how we protect information by first asking the question, "Why in $DEITY's name am I obtaining or storing this in the first place, and is there a reasonable alternative to doing this myself? If my core competency as a retailer is retailing, supply chain, and marketing, why in the world would I run a payment processing environment?" Those are the questions that we need to be asking, and we need to be prepared to train the business on how to act in this brave new world.

FOOTNOTES

[3] *And GOOD testing here, folks. Not checkbox audit testing.*

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