Herding Cats:
The Business of Security

March 2010

BrandenWilliams
SECURE BUSINESS GROWTH

Here's a quick poll for all you readers. Who out there has MORE security resources (financial and human) than are needed to operate an efficient and effective information security program?

(Wait for it…. Hrm… all I hear is crickets. And not just because I can't hear you through the tubes.)

If you were posing as a cricket so that the rest of us would not glare at you, bra-vo. You are either doing something very right or something very wrong.

For the rest of us, we constantly fight the battle of doing what is right over doing what is minimally required and funded. If you don't believe me, let's take a look at why we do SAS-70 audits or PCI DSS assessments. We certainly have not been doing them in support of a larger, mature security architecture program. Maybe a few of you have, but see the paragraph above. You must be one of the few doing something very right.

Both of the aforementioned activities usually are driven by a compliance requirement, an audit finding, or marketing and sales for use as a competitive differentiator. The latter one is one of my favorite justifications for an audit as it is the perfect embodiment of the colloquialism, "put the cart before the horse." If these activities are instead done in support of a larger security framework, that's when it truly becomes a competitive differentiator, and the horse and cart are in the right order.

I've often said that we security professionals are not doing enough to partner with areas outside of our direct control (or influence). Specifically, we do a poor job at helping the business side understand why our initiatives are important (imperative, even), such that we do have adequate resources to accomplish our goals in a reasonable timeframe. The main problem is that we do not have realistic expectations on what is "adequate" and "reasonable." Or, if we do, we are not communicating those effectively such that the business just sits back and says, "OK, where do I sign?"

Effective security management requires a business approach and good relationship management with all levels of management to ensure that CISOs are not treated as the weaker, more feeble sidekick of the CIO. It's easy to be the guy that squawks about "you should do this," or "you are doing that wrong," or screams "I TOLD YOU SO!" immediately following a breach. But nobody likes that guy. The measure of our success should be more than "we've been breach free since 2003.[1]" If we figure out how to deliver value back to the business, we ensure that some other guy's budget gets cut before ours.

In the last several years I have met many CISOs that have a business education (or background) that are taking their turn at figuring out how to run an efficient security function inside a quarterly driven, cost neurotic company. Ironically, it might be easier to run a security program inside of a smaller, non-public company than inside of some of the greatest global corporations. In the big companies, you need someone who understands how to build relationships and the inner workings of corporate P&L management watching over your security function.

Fighting for resources is part of any executive's job, and not something unique to the CISO role. The more successful executives are ones that align themselves with the revenue side of the business (as opposed to cost), and do a better job negotiating their share of

FOOTNOTES

[1] *Ted Moseby, Architect.*

the P&L. Successful CISOs will be able to do both of these.

Should you find yourself in the role of a CISO, your goals for working the business side are fairly clear. The better you can navigate the normal corporate planning process, the more likely you will have the resources you need to keep your name out of the news (at a minimum). Consider taking a class on negotiation or corporate finance. It will serve you well as you chase the rats around the course, and will make you a more rounded executive or manager.

Those classes are not just for executives either! Managers have to negotiate part of the P&L for their projects too. Even individual contributors benefit from learning more about the business and grooming themselves for the top spot.

Security is a business problem. To fail to treat it as such will forever keep you as a thorn in the CIOs side.

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/.

TEL 214 727 8227
FAX 214 432 6174

BLOG brandenwilliams.com

EMAIL brw@brandenwilliams.com

BRANDENWILLIAMS
SECURE BUSINESS GROWTH