Herding Cats:
Practical Security Tips for a Wacky World

May 2008

BrandenWilliams
SECURE BUSINESS GROWTH

This month's topic popped into my head after meeting several CISOs frustrated with their inability to push their initiatives through. It seems as if it takes a major breach to remind the business that security is not just some insurance policy with ever increasing premiums. Security is vital to an organization and should be considered a value add.

Even in high profile breach investigations there is evidence of security staffers begging for basic controls. It just seems like the message is not getting through.

How do we resolve this? How do we turn painful (parental in some cases) discussions about security into a collaborative approach to business growth? I believe the answer lies in our attitudes as security professionals. We need to change our outward focus to that of a customer service initiative.

I cannot take credit for this idea, and I am certainly not the first to approach security this way. I was exposed to this way of thinking by one of my mentors, Randy Kaeder.

We were working with a prospective client that had a non-existant security function when Randy suggested this approach. Their program was in its early stages and they were facing a lack of support from senior management. We armed the CIO with all the appropriate data on similar companies spend, and helped him spin it as a customer service initiative.

Instead of being the bad guys inside of a company, we should think about being enablers. There are plenty of other functions inside a company that have the "bad guy" mentality. Ultimately, if we are not contributing to the bottom line by fueling secure business growth, we allow ourselves to be victims of a layoff when times get tough.

Or worse, when the breach occurs we are viewed as the "I told you so" guys, and we have to live out the rest of our careers remembering how it happened on our watch.

How can we be the good guys with all these regulations coming at us? It seems impossible to cope with an upset Oracle DBA who is forced to scramble and patch his production servers within thirty days of the dreaded quarterly release. Dictating standards can give us the appearance of parents setting up rules for their kids, which will impede our progress every time.

We become the good guys when we change how we interact with the business and become problem solvers. When it comes time for a new initiative, be the person who will help fix issues by coming up with creative solutions that will meet the requirements of both security and the business.

I am reminded of a topical scenario in today's retail world. A client of mine approached me the other day about a wireless Point Of Sale (POS) initiative the business was pushing. Before dumping on the idea, we should come up with ways to do this securely to ensure our data and networks are protected. Less "No Soup for YOU!" and more "You want fries with that?"

A savvy security professional will quickly realize the secondary benefit of a wireless POS. Skimming activities would likely be reduced as the credit card would never leave the sight of the customer! By approaching it in a manner where their problem (implementing a wireless POS) becomes a "we" problem, you can ensure that the needs of the corporation are met securely.

This type of change can only work if your company has a basic security framework in place and a solid governance structure. If the security team is an enforcer of governance, I suggest pushing that activity back to the internal audit team. It is their role to ensure that a corporation is complying with internal and external governance. Let it be our role to address findings in a way that does not impede business or undermine corporate governance or be the bad guys.

You will know you are successful when the business comes to you with their security problems (Bob, I just discovered a server with ten thousand social security numbers on it, what do I do?) as opposed to trying to hide it and perform CYA activities in the case that the big breach does occur.

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 at 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