Herding Cats:
Breaches Can't Happen to Us

July 2011

BrandenWilliams
SECURE BUSINESS GROWTH

Security and business are not terms often placed near each other in print or in conversation. Well, unless you read this column, that is.

I enjoy exploring the concept of security as a business problem, and evidence of security supporting the business in a valuable way. Neither of the two groups bears the full responsibility for a breakdown, but each has their own role.

For example, the information security function of a company has evolved from the crew of misfits randomly poking around the network in a way that doesn't take it down relegated to a dark corner in the basement with no windows. It's not the bastard child of IT. It's not audit. It shouldn't just be a cost center[1]. It's a thread that is woven throughout the fabric of the business, whether we view it that way or not. In your organizations, security should be enabling the business to run well, securely. It's our job to communicate this message and ability back to the C-Suite, such that we have a seat at the table during the strategic discussions and decisions that frame the current and future states of the business.

On the flip side, the business has a strange view of risk management in general. When bad things don't happen, the business starts to believe they CAN'T happen, which causes them to take more risk at a much higher price when things go wrong. You don't have to look very hard through news articles to see examples of this all throughout history—most recently with the global financial crisis. I've worked with several companies and executives after those bad things happen, and one of the first things they ask me is "How in the world did we end up here?" It's not entirely the business's fault; we security folk haven't figured how to quantifiably measure risk in a way that is transferrable from one company to the next. When we can't really measure something, we start filling in the gaps with assumptions that end up dramatically skewing our view of the end risk.

Think back to the last time you put together a risk model to justify some security spend. What did your assumptions look like? Did you use the old Annualized Loss Expectancy model to put together those numbers? Did you compare your company's spend on security with an approximation of your industry? Was it well received by the holders of the purse strings? Before you asked for new funding, did you analyze how you were using your current assets and operating expense plans for the year to make sure you were allocating your existing resources in a way that maximizes their effectiveness?

I imagine that you answered yes to some, no to others, and probably differently from each your industry peers.

In order to run a successful security function in the business, you must treat it like a business. Sure, it will have some kind of cost center associated with it, but it should be run like a traditional Profit & Loss (P&L) business function. Do you know who your customers are, how much money they pay you for your services, and how you make the best use of that money to deliver value back to your customers? And just like other vendors, do you measure your effectiveness with metrics to show your customer the value of their investment?

Based on what I see in my customers, the answer isn't positive. Sure, some are well run, but the vast majority flounder[2]. If you can't easily pull together answers to questions in

FOOTNOTES

[1] I'm not talking ROI, I'm just saying that to be relevant to the business, it must find ways to deliver value.

[2] It's like taco.

the preceding paragraph, you are yet another area of the company that is treated like a cost center and will likely face cuts the next time your company's finances get into trouble. Your CISO must understand the constructs of business, understand how to run a P&L, and have the power to allocate resources in ways that he knows will be the most effective. If the only measure of your success is the lack of a breach, how long until your executives think a breach can't happen to them?

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