Herding Cats:
Walk that walk!

August 2011

BrandenWilliams
SECURE BUSINESS GROWTH

The business aspects of security have become one of my favorite topics both here and in my blog. In my experience, people talk a big talk when it comes to treating security like a business, but they don't walk the big walk. I'm not saying it's easy, but then again, nothing worth doing is!

Of course, "walking the walk" has to happen at some point because most companies live by budgets and planning. At some point, a business person is going to ask us how we justify the rate of spend we have in our department. That's where security architecture comes in, as it often is the blueprint that allows us to get to that grand total of spend. Then it is back up to the business-savvy CISO to take the results and ensure that we are protecting the right resources with the right amount of security, and doing it efficiently.

Before you can architect any sort of security plan, you truly must have a solid grasp on how the business operates, and what specifically your company does for the revenues it earns. Imagine for a second that someone contracted you to architect a security system for a house. How would you build that security system if you didn't know basic things like the size and layout of the house, what the neighborhood looks like, the kind of people and businesses are around, and the contents inside the house you are trying to protect? You would protect a single-story ranch home with a single television and basic furniture much different from two-story McMansion where every room has a flat-panel TV and the lady of the castle has $100,000 worth of jewelry in her dresser.

Take that same analogy and apply it to your business. How much money should you spend on hardware, services, and operating expenses to keep the security function running? You can't possibly know that until you have a good working knowledge of how the business operates.

The good thing about architecting your security function is the number of generally accepted resources available to you to adapt and repurpose. For example, if you are starting from scratch, you might check out NIST SP 800-12 and 14 (albeit dated), and then potentially move to SP 800-39. I'm not just making up numbers, I'm pulling these from NIST's Computer Security Division's listing of special publications[1].

These publications are great for two big reasons; first, they are free, and second, they provide a wealth of information that far exceed the basic parts of your entire security strategy. They get as broad as the ones I mentioned above, and as narrow as SP 800-135 which is titled, "Recommendation for Existing Application-Specific Key Derivation Functions." If you have not perused these publications, go check them out now. They are not the panacea for security problems, but they can play a critical part in your ability to serve the business.

Once you fully understand the business, you have an opportunity to help shape the business's operations. For example, you might discover some kind of data sitting around that is highly regulated and expensive to protect. If the business tells you that they only collect this data incidentally, you may be able to help them discover a better way to operate and completely wash yourself of the need to protect that data. You aren't working yourself out of a job, you are demonstrating your true value to the organization by checking to make sure the parachute is packed correctly. Your value is not apparent by telling the board how many new firewalls you added and now manage; it's showing them

FOOTNOTES

[1] You can see these and many more by browsing here: http://csrc.nist.gov/publications/PubsSPs.html

how to securely operate and grow their business without them.

Remember, security is a business problem. You certainly would not employ the same methods and tools to protect a standalone manufacturing facility as you would a regional trucking company. That's why it is critical that you understand how the business operates, how they make money, and what critical areas will potentially affect your paycheck if they are damaged, destroyed, or rendered inoperable for a short period of time. Architect your security around those functional areas and offload the rest of the risk to someone else.

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/.