Herding Cats:
Governance is a Party

December 2011

BrandenWilliams
SECURE BUSINESS GROWTH

I bet you are ready for a ho-hum piece on governance, aren't you? I mean, those governance guys… PARTY ANIMALS!

Governance, besides being a three syllable word that people yawn more than they speak, is one of those things that is not only critical to the success of your organization, but includes parts of your day to day job probably without you even thinking about it. Governance sometimes comes in the form of all those spreadsheets you maintain[1] for auditors. In the corporate world, it can come in the form of policies, standards, guidelines, and procedures. Those things aren't just designed to keep you in line as a lowly worker—they also can help promote efficiency, consistency, and overall quality of a product or service. Companies build governance programs to comply with laws, limit liability and insider fraud, and enable trust in partnerships throughout the supply chain.

But if virtually everyone has some reason to have a highly functional governance program at their company, why do we all roll our eyes when someone talks about building some flashy technology to show it off? Surely we wouldn't redirect budget from a GRC project to a flashy security tool that will help some aspects of our lives.

Right?

I've been in the information security space for a long time now, and I've seen all manner of really awesome technologies be born, reborn, deployed well, deployed poorly, replaced, and shelved. For the most part, every one of these security tools has operated independent from the business side of the house. Sure, they may have been extremely cool, but they never had real traction with any business person in your company. Imagine trying to explain the merits of a Layer 7 firewall over a traditional Layer 4 one to George in Finance. I bet it probably went over better in your head than it would in real life.

One of the main reasons why governance has gained tremendous momentum over the last few years is the virtually uncontrolled explosion of laws and compliance regulations companies are now subject to as they collect and use information about their customers. Any company required to demonstrate compliance with any substantial amount of these laws is at an instant disadvantage if they are manually tracking events. Small partnerships may prefer a manual method over investing in a software package if their requirements are manageable without workflow management and automation software. Others may ignore it until they suffer a breach and then find someone to blame.

Governance has become so popular over the last five years that an entire industry has flourished, including with several acquisitions whereby small, innovative products and services are added to larger a company's offering. Once joined with larger enterprises, it allows the GRC (and sometimes security discussion) to be brought into the boardroom of large enterprises. Executives don't typically talk security, but they do understand controls.

Now imagine a situation where the business is driving an initiative like controls around electronic employee data. You might think that it sure looks like an information security project. I might call that a governance program, or some folks might call it GRC. Regardless, this is something being driven from the business side of the house, and we are well poised to assist. The tools typically used to track GRC programs today are pathetic. Spreadsheets and basic desktop databases have their purpose in business, but managing functional GRC

FOOTNOTES

[1] *Or update right before the auditor shows up, as it were.*

programs isn't one of them. Unfortunately, this is probably the only tool the business folks have access to and can operate it in a manner that meets their perceived needs. Imagine trying to build a sleek and scalable firewall by coding exclusively in BASIC. I'm not saying you COULDN'T get it done[2] but you are going to have a much better time working with a more structured foundation.

The governance discussion is one of the few where a security person can walk into the office of a finance person and both can work together toward a common goal—building tools and processes to reduce the financial impact (by time and resources) external forces place on our operations. If you have been looking for a way to start building relationships into the business, here's an easy one.

FOOTNOTES

[2] *CHALLENGE ACCEPTED!*

About the Author:

Branden R. Williams, CISSP, CISM, 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 the 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