Herding Cats:
Crushing Cross-Dysfuntionalism

October 2008

"GUILTY!"

The peanut gallery gasps as the verdict is forcefully read by the foreman, then erupts in a chorus of "RABBLE-RABBLEs." The CEO (defendant) humbly bows his head as he rises from his chair, waiting for the bailiff to claim his freedom.

In the case of information security, we've seen major breaches; but no CEOs of major companies are heading to jail because of it (unless they were involved in the fraud). Could a CEO be hauled off to jail for neglecting to assign and elevate the significance of information security? Unlikely, but wouldn't it be an interesting world if they could?

Today's large IT organizations generally operate as silos. Developers write applications. Provisioning groups deploy systems. Security Risk Management chooses which patches to deploy. Infrastructure designs and maintains networks. Geographic groups function within their time zone and border. Not only do these groups lack fluid communication, but they often make decisions inside their silo that affects others.

Managing change is one of the biggest headaches that compliance organizations face. I often visit companies that were previously compliant with one particular standard, only to find that poorly managed change has pushed them out of compliance. Compliance with most standards is a daily battle, and cross-dysfuctional teams[1] often overlook minor issues that become gaping security holes.

For example, let's say that an application developer uses a some third-party ode that contains a known vulnerability in a particular service. Developer thinks, "I don't have time to upgrade this third-party code because the new version has other changes that break my code. It shouldn't matter anyway because the infrastructure group has firewalls protecting me." Fairly innocuous if communicated in that way.

But now let's say that one of the infrastructure gals is reviewing a change request from another group that would require opening a particular port in a firewall. That port in question is standard, but would expose the vulnerability in the third-party code the developer is using. She thinks, "I just manage firewalls. The appropriate documentation for this group is here, so I'll make the change. Besides, it is the developers' responsibility to write and use non-vulnerable code."

BAM! Even Emeril can see that there is a high potential for a breach.

In the last issue, Alain Mayer writes, "the problem with managing change is that it is handled by disparate, silo-oriented functional groups."[2] It is actually worse than that. Change control has become such a pain for some companies, that they have moved to silo-oriented change control meetings instead of one large change control group! Reviewed changes should include all relevant areas, and changes made inside silos rarely do.

What we need to do is start **busting** these silos.

In Silos, Politics, and Turf Wars: A Leadership Fable About Destroying the Barriers That Turn Colleagues into Competitors, Patrick Lencioni argues that silos arise because corporate

---

FOOTNOTES
[1] Waife, Ronald S. "Cross-(Dys)Functional Teams." Applied Clinical Trials Online, August 2002).
[2] Mayer, Alain. "Security Risk and Overcoming IT Silos," ISSA Journal 6, no. 9 (September 2008): 10-12.

BRANDENWRITES

leaders fail to "provide themselves and their employees with a compelling context for working together."[3]. Many managers end up contributing to the silo problem simply by trying to preserve their way of life for themselves and their team. This creates cross-dysfunctional teams.

It doesn't take a rocket surgeon to see that silo busting must come from the top of an organization. If the CEO is not interested in busting silos, there is little that the security group can do. However, security must rise above the dangers of cross-dysfunctional teams by remembering the goals of the organization.

Is it your company's goal to achieve only the absolute bare minimum required by law or regulation? Has your company suffered a breach (or do they just "get it") and realize how important information security is to the longevity of the business? If it is the former, I fear that your frustration will only continue. If it is the latter, it is time to start building relationships with managers of groups that can impact your company's security posture. Understand what they do, what their constraints are, and find ways to educate them on security so it becomes part of their daily work routines.

Only then can you begin to bust those silos and put the "fun" back in cross-functional teams.

FOOTNOTES
[3] Lencioni, Patrick. _Silos, Politics, and Turf Wars: A Leadership Fable About Destroying the Barriers That Turn Colleagues into Competitors_ (Jossey-Bass, 2006).

Brandenwrites

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 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