Herding Cats:
Risky Business

January 2013

BrandenWilliams
SECURE BUSINESS GROWTH

It's 2013, and I can't think of a better way to start off the year than to review how we ended up here. And by ended up here, I mean still exist. Remember that calendar thingie that corresponded with the winter solstice last month? If you are reading this, then WE SURVIVED! Did anyone you know take the date seriously? Were they sitting in their bunker waiting for the rain of meteors that never came? Let's compare this whole scenario to risk analysis and management.

Back in the 1960s, a scholar by the name of Michael D. Coe explained that the completion of the long-calendar cycle suggests the end of the world as we know it. Of course, it wasn't until the last two years that we've seen any real attention payed to this statement, but it has since been refuted by a number of current scholars. In risk analysis terms, Coe identified a risk, and performed a brief analysis in the 60s, where current scholars did further research and analysis to conclude that it was nothing worth spending time on. Once recent scholars completed their analysis, current risk managers could then manage the risk through conclusion—it isn't a "black swan", it's a unicorn with mind control powers (I.e., it's more probable that you will win the Powerball multiple times over).

But not all risks are quite this easy to dismiss. For example, Hurricane Sandy identified some faulty risk management assumptions (or simply unidentified risk) for companies with data centers below 34th Street in Manhattan. Obviously, some risk managers did not think that a super-cane would sweep up the coast and target that part of the country, otherwise they would have put some backup systems in place to ensure that their services did not get interrupted. Regardless whether it were company providing news services like Gawker, or a power company operating a local substation, if it was important to remain up all the time this is a risk that should have been analyzed and managed.

Now, not all risk management techniques would have resulted in a different outcome. For example, as easy as it is for me to argue that these outages are a result of poor risk management, I could argue that they were superb risk management. The reward of offering services in these areas may have far outweighed the risk of a week or two of downtime (or the cost to prevent it). Risk managers may have identified the risk after watching "The Day After Tomorrow" and presented it to management, but their decision after weighing all of the pros and cons may have been to accept the risk as-is, and deal with it when it happens. So many people change jobs on a frequent basis that it can be easier to assume the risk (knowing that the chances are high it will be someone else's problem in five years) than it is to address the risk.

It's certainly cheaper.

And with risk management continuing to be debated with a growing body of knowledge surrounding it, it's becoming more difficult to expand it beyond a basic financial impact. Information security makes this problem worse because risk managers often don't understand the intricacies of the vulnerabilities associated with a spread-out IT posture. Think about this for a minute: companies don't control the networks (mobility), infrastructure (cloud), or device (BYOD) anymore, yet they are still charged with protecting all of the data they use, store, and access!

But, all is not lost! Even with the somewhat vast and confusing amount of theory on risk management, there are still ways that we can do a better job of addressing the risk process within our companies. The first step is for our information security and risk management professionals to assume more of an active role in understanding how the business operates. This requires uncomfortable, face-to-face conversations that might normally not happen. Understanding all of the nuances in the business is like putting on a pair of corrective lenses over nearsighted eyes. This clarity will help you better identify which risks are real, which are of low probability of occurrence, and how you can create a system to keep those up to date to manage them.

Will you have arguments as your company tries to define and address the identified risk? Certainly. But that process (if productive) will force top leaders to come to grips with the landscape of risks in terms they understand—its relation to the business.

Contact information for requests for permission to reproduce or distribute materials available are listed below.

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 speaker 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/.