Herding Cats:
Trust in the System

September 2011

BRANDENWILLIAMS
SECURE BUSINESS GROWTH

The general user's comprehension of trust in computing is becoming more implied as we more and more of our lives are digitized. The reality is this couldn't be farther from the truth.

Many young people feel the sting of a breach of implied privacy from social media postings reaching farther than intended. If you look through my blog, you will find a few posts that have examples of people getting burned from social media postings. Be it an errant post on Twitter that cost someone their new job or a geo-tagged picture that reveals a location that should have been kept secret, lives have been changed for the worse because of misguided trust in the system.

I am included in this group. I am amazed at my change in attitude over the years. I prefer convenience; and if that means you will get the privilege of storing my information to make life easier, I'm probably going to let you store it. After all, I'm protected, right?

Fifteen years ago I was wary of digitizing certain parts of my life. I saw how companies tried to operate their infrastructure, and saw that functionality was much preferred over information security. In many cases, it still is today[1]. My time spent as a system administrator taught me that there is always someone of equal or higher permission on a system than me, and everything I digitize can be accessed by someone else. This experience stunts my own usage of certain cloud services like cloud-based backup and recovery, and parts of the new iCloud service[2].

As I wrote about last month, we are undergoing a revolutionary transformation in how we provide IT services to our customers. The move to the cloud, virtual data centers, and utility computing allow us to turn our IT centers into businesses because we can more directly measure the cost and margin associated with providing services[3]. This stuff really excites me because I love digging into numbers in spite of barely passing my undergrad accounting classes. Imagine for a moment that you could quantify exactly how much it costs you to process an order on-line. You could figure out how much computing power is used in the shopping process, optimize the customer experience to reduce the amount of time a shopper spends browsing, and know the exact margin[4] from that transaction. On demand discounts for quickly navigating to your product and completing a purchase? Now that's using system data to your advantage!

But how do I know that cloud resources will be there when I need them? Can I afford to put my company's livelihood in the hands of a service provider? Can I trust the service provider to safeguard my intellectual property and customer data so I won't have to explain to my shareholders how a data breach occurred on my watch?

These are the questions facing CIOs moving to utility computing today and this is the element of trust they face. This movement creates even more architecture and design questions nowhere near the traditional definitions of information systems or of trusted computing. What it seems is that service providers have not quite stepped up to the security plate, and the larger they are, the less liability they want. No CIO should bank on compensatory damages after a drawn out lawsuit to replace cash spent cleaning up a breach—and CIOs that do should be immediately terminated.

FOOTNOTES

[1] *See the cloud!*

[2] *Check my blog for more on the security issues with iCloud.*

[3] *If your company still refers to IT as a cost center, you are living in the old world of IT.*

[4] *The amount of profit you earn.*

If you are looking for ways to make your move to the cloud, the first thing you need to do is consider what you are moving to the cloud. Regulated data has no business with most cloud providers, but unregulated data is fine. Next you need to very closely examine the contract with that provider. Buddy up with your lawyer and fully understand where the responsibility lies for security and the types of damages you may be entitled to if you are on the hook for a breach. Finally, look for reasons to trust your cloud provider. Do they dodge questions about security, or use the wrong acronyms? Is their auditor ABC Audit Co[5]? Trust the provider before you entrust your data to it.

FOOTNOTES

[5] *Which may be a fine establishment.*

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

<u>About the Author:</u>

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/.