Herding Cats:
No Bubble People

February 2012

BrandenWilliams
SECURE BUSINESS GROWTH

February is not really the time when we make predictions about the coming year—that's reserved for December. But this month I want to talk about a topic that will see increasing importance in 2012. It's the intersection of Big Data and information security. 2012 is the year of the hunter, and Big Data is a critically important arrow in his quiver.

Last year was bad for the "good guys." Hactivists, nation states, and organized crime syndicates clearly made their capabilities, if not partially their intentions, known to the world at large. It's 2012, and it's an exciting year to be a security professional. Many of us are making our way into the board room and rubbing elbows with some powerful people. It's even coaxing some of our introverted brethren to become more social. The best part? CEOs finally are paying attention to information security!

But our security futures aren't based in firewalls, cloud security, and compliance, they will be shaped by our ability to perceive threats against our informational assets in real time. We won't be called upon only after bad things happen, we'll be expected to prevent them from happening—probably without many more resources than we have today. Big Data will power our perception, but only if we can hone our skills, build real-time and relevant analytics, and adjust our posture and asset protection on the fly.

The relevant security slice of Big Data will help us identify threats before they manifest themselves in a breach. We want to be able to move our actions further to the left on the kill chain. We also will have to concede some battles to focus on fighting the war. For example, we may have to assume that our users will click on links that introduce malware into their systems. But we don't have to assume that a malware infection immediately and always leads to exfiltration of data (i.e., a breach).

Let's say you have an informational asset in a critical system and the manufacturer of that system identifies a security vulnerability that should be rapidly patched. Once the vendor announces the vulnerability and patch, you can bet that proof of concept code exists to demonstrate the exploit. If you were a target during that timeframe, there may be some weaponized malware out there. Are you a target? Is that information valuable to someone else? Is it valuable when it becomes lost? With Big Data, you might be able to not only understand which employees would specifically be targeted by an outsider to assist in a data breach, but you could even see the attack in process and stop it before exploitation or command and control happens.

There is simply too much malware out there to be strictly focused on keeping your users infection free. They would become the modern corporate equivalent of "bubble people" whereby they can only interact with the world from a sterile environment. It's impractical, and frankly impossible when you look at how business operates. Instead, you provide them with hand-washing education, the basics of how infection works, and rounds of anti-viral and antibiotic remedies when they do catch the common cold. Assume your users will get infected, but don't assume infection means loss.

Big Data can help us manage our systems better as well. Not only do we need to automate our ability to do massive policy changes based on the threat landscape, but we need to create a mechanism to correlate known assets with real-time threats. External intelligence is critical, and it will come from a variety of sources. You will not only buy relevant intelligence for your industry and company's assets, but you will use freely available sources from social media to determine geopolitical forces and the potential for hacktivism against your organization. It's about correlation and real-time analytics that provide you with actionable intelligence.

2012 will be seen as the year whereby security professionals turned a corner in their abilities to really be effective in protecting their companies and themselves. The groundwork we do today will lay the foundation for our capabilities to learn, protect, and react to changes in the forces that act upon our business, and do it in a way that protects the business and ourselves.

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 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/.