Herding Cats:
Infosec Follies

October 2012

BrandenWilliams

SECURE BUSINESS GROWTH

Here's a hot sports opinion for you: I think our industry is terrible at information risk analysis and management. There is a significant gap between what information security professionals consider high risk and what business professionals consider high risk. I've been in those meetings where information security has had their legs cut out from under them, but I've also been in meetings where open checkbooks for security were passed around like month-old Halloween candy[1]. There are a number of reasons for this; let's explore a few here.

The most glaring omission is our repeated usage of inaccurate (or inconsistent) historical data. If we are terrible at forecasting when and where events will occur and their impact to our business, we look no better than the sales person who forecasts a 75% miss in the last week of the quarter. So we take an ultra conservative approach to try and cover our bases. There are a bunch of you out there who have done this successfully for a number of years, and so far you haven't been bit. There used to be an old saying (which probably still exists in some circles, but I'm going to pretend it doesn't anymore) in the PCI DSS compliance world that went like this: "You are compliant until you are compromised." Meaning, it didn't matter what you reported to your processor as long as you were breach free. The moment that breach hit, however, you were in a world of hurt as your misrepresentation of compliance status came to light. In many cases, you are great at risk management until you are exposed by a poorly managed risk. Complacency begets carelessness—don't expect that this state to remain constant forever.

Another problem is our ability to properly judge the value of our information as it relates to its value to you, its value to a competitor or military, or its value once the data is lost[2]. Risk professionals don't take into account the differences in value when you consider these elements, and attackers will congregate where significant difference exists. If you need examples of this, ask yourself why many companies store live credit card data after a transaction has settled. The pressure PCI DSS compliance applied to the processing and acquiring community ultimately rendered that data useless to merchants after clearing. For those wanting to perform analytics, that's where tokens come into play. All analytics are intact with significantly reduced risk, so why do companies refuse to give it up? That's a question for another column.

Of course, much of this doesn't matter anyway because we don't have the visibility into our infrastructure to track data movement and usage. Some of this is because of the growth and usage of the cloud, but much of this is due to a lack of budget or resources, both of which can be attained with more effective communication.

Finally, we have a terrible time communicating risk outside of our close-knit group of security professionals. It's the worst inside joke. We all seem to know what the risks are to our environment, but for whatever reason they don't match up with the business's interpretation of the same risk. This is pretty easy to solve (probably the easiest of the problems listed above) because it starts with honest communication between risk, legal, IT, and infosec—a true collective understanding of the business and how it operates.

So how do we get better at this? After we create our coalition of internal risk champions and outfit them with superhero uniforms (no capes!), we have to take a serious inventory

FOOTNOTES

[1] This usually happened after a significant security incident whereby the true business risk was exposed. Ironically enough, neither the information security nor the business had the risk levels right.

[2] For more information, watch blog.brandenwilliams.com in the coming months.

of our information assets; their locations, acquisition, use, and disposal procedures; and we have to take a serious look at the threat actors that want to steal that information whether it is an insider, hacktivist, organized crime syndicate, or nation state. Now that we have a better idea of the threat actors and what they want, we need comprehensive visibility into our infrastructure coupled with actionable intelligence from the outside that helps us determine where we need to focus our resources. Then, with all of this together, we can start making rational decisions about what data we keep, what we dump, how we use it, and most importantly, how we protect it.

<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 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/.