Herding Cats:
Risk Management Follies

September 2009

BrandenWilliams
SECURE BUSINESS GROWTH

It seems like until the last decade, we mostly used the term Risk Management for financial purposes. How much "risk" is in X business line, or Y investment? Once information technology began driving our businesses (as opposed to a neat toy the CEO could use to impress investors), risk management had to be expanded to include those systems and their impact to the business.

Calculating risk has evolved over the years. Most security texts are quick to reference the Annualized Loss Expectancy (ALE) formula as a benchmark for the most amount of money you should spend securing an asset in any given year. The formula takes the Single Loss Expectancy (SLE), or how much it would cost to address a loss of the system or asset, and multiplies it by the Annualized Rate of Occurrence (ARO), or the probability of the system or asset suffering a loss during a one-year period.

$$ALE = SLE * ARO$$

In the last ten or so years, an increasing number of people have come out against the ALE formula from both the security and business side! So much so that I would argue the formula has become polarizing in some respects. Some individuals live and die by it, while others avoid it like my wife avoids talking to me while the Dallas Cowboys are playing[1]. I'm on the avoiding side, for a few reasons.

SLE is often miscalculated. When you deal with a formula that only has two elements in it, a minor miscalculation on one can dramatically impacts the result. Traditionally, SLE attempted to calculate the "loss" element from a downtime-and-rebuilding-the-system standpoint. It DIDN'T account for the legal impact of losing data (albeit, that is much better defined today), and anyone who tells you he can estimate how much any data loss might cost is selling you snake oil (you know who you are).

Don't believe me? There have been at least three public U.S. companies breached in the last three years. Go look at their financial statements and tell me if you can find a pattern worthy enough of distilling into a quick and dirty dollars-per-record cost.

The other element, ARO, is based on probability. I'm not a math whiz (and neither are most of the people calculating this value), so what makes me think I can use complex concepts of applied mathematics with any accuracy at all? If you goof up your probability by say 10%, your results could skew wildly.

Try this exercise. Find a few security or audit people in your organization, and ask them to calculate the ALE for a group of assets. If you were to perform a statistical analysis of the results, how big would your standard deviation be[2]? My guess? Pretty big.

It's no wonder the C-level risk managers (read CEO, CFO, CIO, CTO, COO, and other board members) have no concept of what kind of security resources to deploy in their organization. We've been feeding them guesswork data for YEARS!

I think the retrospective look on breaches tells us one thing: we cannot trust our estimates.

FOOTNOTES

[1] Unless it is to comment on the game specifically, which she does from time to time. Although, wife, please quit screaming "IT'S A FAKE" every time they punt just so the one time they do, you will be right.

[2] For this exercise, your standard deviation would be dollars. Smaller standard deviations mean that everyone ended up with pretty much the same result.

So what do we do? Do we ratchet up security spending until it is woefully out of control? Do we just give up on security?

Of course not! We have a few things to do. First, we need a solid and proven risk assessment methodology. Until ISO 27005 is released, we have to go back to some of our oldies, but maybe still goodies. ISO 27002 has a small risk assessment process outlined that we could follow, or we could try NIST's SP800-53A[3].

The basic answer starts with finding out what data you store, how valuable it is to a criminal, and how much you actually need. Destroy everything you don't, and fight to the death to secure what you do. NIST's SP800-39[4] (in draft form) suggests just that. Step 1: Categorize your security systems; Step 2: Select security controls; Step 3: Implement security controls; THEN Step 4: Assess security controls. So often, especially with PCI, we try to put the cart before the horse and implement controls on systems before we know what is on them.

Maybe if we stopped to focus on the information we are trying to secure, we'd be more successful in securing it!

FOOTNOTES

[3] *http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf*

[4] *http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf*

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