Herding Cats:
The Breach You DID Expect!

May 2009

BRANDENWILLIAMS
SECURE BUSINESS GROWTH

Call it being lazy, or call it part of the brilliant master plan. I did think about this issue when I was writing the March issue. This month, we will explore the good old standard breach that you do expect. Or, maybe the one that you should expect based on the poor economy.

If you are unlucky enough to suffer a breach during an economic contraction, expect cleaning up after it to cost more. Notice I did not say that you pay more for a breach during an economic contraction. The word choice is on purpose, and a key nugget in the message that we all need to tell our management.

If your company suffers a breach in 2009, it will cost more than if it suffered one in 2007 or even 2008. 2009 is the year of a weak economy, shrinking GDP[1], and flat or declining cash reserves and growth. Many companies are so leveraged that the term 'cash reserve' is something their employees have only read about in an MBA finance class. Companies are in preservation mode, and will do whatever they can to survive and be well positioned when things turn around.

"Hang on one minute," you ask, "didn't you just write about this two issues ago?"

If you were to ask Mr. CEO if he would spend fifty-million dollars over the next three years to improve security, comply with the laws and regulations, and significantly reduce the risk of answering for a breach, most of them would say "Nah." Without context, security spending can look frivolous in a weak economy. "It is not something we need to make the lever go 'plunk,' so why would I spend money on it?" That line of thinking, while technically correct, is short sided. The correct question is would you spend it to make sure that there still is a lever, and it still goes 'plunk'?

Here is a proverbial fork in the road story. On the the path of leadership, every CEO will reach a fork. The path to the left looks like the scenario painted above. The path to the right is the scary path with rapids, or dark woods, or spiders in the closet, whatever makes you fidget with fear. The path to the right is the $200 million that must be spent in eighteen months (or some other short period of time) to clean up after a breach.

Now you tell your CEO that he must choose! It's an either/or situation. He can set up camp at the fork in the road as long as he likes, but someday, the swift kick of a breach will boot him over to the right where shareholder value evaporates overnight.

Several public companies have suffered breaches in the U.S., and anyone with a basic understanding of accounting can calculate most of the money allocated to clean up and recover from those breaches. Money that was used to show a healthy financial ratios on the books, or the cash reserve to weather an economic storm, or to invest in growth.

"But Branden," Mr. CEO says, "what is the probability that this event will actually happen? If I don't need to spend fifty million, I won't." Ahh yes, the age-old probability question. That's why we created all these fancy formulas like the Annualized Loss Expectancy, right? So we can work this vacuous problem of figuring out how much money to spend on security?

The probability question pains us. CEOs don't understand what we do, and the only way we've figured out how to talk to them is through vague formulas that don't articulate the

FOOTNOTES

[1] Or GNP, but let's not argue semantics.

issue. Therefore, CEOs treat us like a cost center and not a strategic investment[2].

The CEO may choose to stay at the fork in the road indefinitely, but the dollar amounts associated with the left and right path will continue to grow. Fifty million this year may turn into fifty-two or fifty-five next year to clean up after more operations where security was not part of the corporate strategy. So instead, challenge your CEO to take advantage of a year of bad margins and profits and invest some of the cash reserves in security!

FOOTNOTES

[1] Please keep in mind that when I use the term 'invest,' I do not mean a financial instrument that will generate return. I am using it in the sense that spending smart now will reduce spend in the future. You can't articulate that until the event happens, and then it's too late anyway.

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

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

SECURE BUSINESS GROWTH