Herding Cats:
What's the Value?

November 2011

BrandenWilliams
SECURE BUSINESS GROWTH

This month's theme tackles the yet-widely-unsolved problem of accurate and effective information risk management. It's unsolved because not only are risks different from company to company and individual to individual, we can't even agree on the monetary value of the information we are charged to protect.

I recently spoke at a risk management forum and used an analogy I appropriated from the great Chuck Hollis of EMC. We have a hard time protecting information because we have a hard time valuing information. Imagine for a second that someone gave you a pile of money, in cash, and told you to protect it. Let's say it was $100,000. I bet you could think of some appropriate ways you could protect that cash, as well as some appropriate expenses you would use during that process. For example, you probably wouldn't spend $500,000 on a vault to store $100,000 in cash. You might use someone else's expensive vault, or you might spend some smaller amount to build an appropriate protection mechanism. When we are dealing with cash, risk management and protection is easy.

Now imagine that someone gave you a pile of information. Maybe it's small enough to fit on a USB stick. Maybe it covers several terabytes of space on a corporate-wide SAN. How do you value that information such that you can deploy appropriate protection mechanisms to keep it safe? Ironically, I can envision that we could potentially arrive at the same dollar amount regardless of the size where data on a USB stick might be worth the same or more than terabytes sitting in a secured facility.

I had an interesting debate with a close friend last month about how data breaches are evolving in numbers and severity over the course of 2011. The number of breaches seems to be decreasing while the severity of the breaches increase[1]. How does this impact our ability to keep sensitive information secure? Some argue that a higher number of breaches at some kind of consistent pace are better for us because it keeps the topic top of mind. I believe that the severity of the breach is more important to get the C-level attention we need over the frequency of occurrence.

Organizations are built to allow for autonomous decisions at various dollar amounts (financial impact) throughout the corporate hierarchy. This means that lower level employees are typically empowered to handle events with small financial impact to keep the big guys focused on the big things. The bigwigs are less likely to pay attention if the impact of the event doesn't surpass their report's thresholds (or maybe even their own). We don't need to spend all of our resources preparing for a Black Swan, but we do need to prepare for the reality that our network is compromised today. The way we go about information security isn't effective anymore because we base our architecture on the concept of trust (often times misplaced in humans).

Designing security controls that match business requirements requires that we both understand the business and can agree on a reasonable value to the information we are trying to protect. Companies today store too much information and carry too much financial liability because of they know neither of those. We should only be storing the information we value as an asset, and find a way to transfer the risk of security other information to third parties. These service providers exist today, but our companies rarely analyze how they use information in their businesses. We regularly perform analytics on what is on-hand, but how often do we ask the question, "Why do we have this data in the

FOOTNOTES

[1] This is a total gut feel on my part. I know half of my gut feel is based on what is reported and what isn't, something Mr. Adamson pointed out to me as we snacked on super delicious Char Grilled Octopus from Keegan's in St. Pete's.

first place?"

Not often enough.

I've had several discussions with customers recently where they have confessed they found information in their systems that they didn't know was there, didn't have a business use for, and found that it was sensitive in nature. This isn't an advertisement for Data-Loss Prevention, it's a plea for diligence. Start there, and then re-evaluate your risk management process.

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/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH