Herding Cats:
Laws, It's CHAOS

January 2011

BrandenWilliams
SECURE BUSINESS GROWTH

We've come a long way since the Computer Fraud and Abuse Act (CFAA) of 1986 which was the amended version of the Counterfeit Access Device Act of 1984[1]. When this piece of legislation was enacted we were still on the leading edge of the electronic part of our information revolution. It's not that we didn't have lots of information in the 80s, we just realized that we needed better ways to analyze, search through, store, and access it. The commercialization and evolution of the computer chips designed in the 60s and 70s, and massive disk arrays such as the IBM 3380 released in 1980—the first commercial storage device with one gigabyte capacity, yours for the low, low price of $40,000[2]—presented a solution to companies looking to make things easier. As the prices came down, corporate America's appetite for storage and electronic information boomed and our habit of using paper began to slowly change to an electronic equivalent.

Fast forward to today. Fewer processes rely on paper-based workflows, and the ones that are left are quickly becoming digitized for fast, reliable access. But with convenient access comes easy and frequent accidental disclosure. Look out world, here comes LEGISLATION!

Legislation on information security is terrifying to me. I've watched enough congressional hearings to know that the vast majority of legislators in the US House and Senate do not have the requisite base of knowledge to do anything more than recite prepared statements from those that are in the know. I understand the challenge that legislators have, but I also realize that criminals change their attack strategies faster than the government can enact legislation to combat the hack of the day. When legislation comes down, it tends to be either sweeping with financial incentives (like HITECH) or watered down with limited concrete detail (like Gramm-Leach-Bliley)[3]. Combine those constraints with fifty individual states that may enact their own legislation to protect their residents[4] and you end up with an extremely complex legal landscape, against which security professionals are regularly measured.

In some respects, we should be glad that someone realized the carrot method isn't working and it's time to bring out the stick. Information Security spending as a component of overall IT spend has grown tremendously over the last decade. Without some legislation and the very public dissection of the legal ramifications of breaches, I am not sure companies would spend much beyond the "Availability" and "Integrity" legs[5] of the CIA tripod. I recently compared the failings of information security to the same issues we have in physical security[6], and even our physical world mirrors the same "It won't happen to me" mentality that information security has harbored since the first computers were operated. If a business gets robbed, a new security system is installed. If a company is compromised, all the sudden executives are serious about all those proposals you pitched over the last decade.

As you readers know, one of my mantras is that we are to blame for the failings of information security in the board room, not them. Our failure to communicate the value and importance in a language that the board can understand has forced legislation upon the private sector to cattle prod those guys into action. Even that does not work uniformly as not every company complies with all of the relevant information security regulations

FOOTNOTES

[1] What a horrible name!
[2] Just over $100K in today's dollars.
[3] Arguably this had more to do with privacy than security, but I saw many financial organizations make changes in their information security activities based on this legislation.
[4] See all the disclosure notification legislation, or the Nevada, Minnesota, and Massachusetts laws.
[5] With a much heavier emphasis on Availability.
[6] http://bit.ly/dUSQXi

on all of the books from every sovereign nation with which they interact. It's painful, and it's only going to get worse.

What can you do? First off, get friendly with a good lawyer that you trust. The information security team should be a good partner with the legal team to better understand exactly what you need to do to stay ahead of, and in compliance with, the legislation on the books. For the most part, it means building a mature information security program based on something like ISO 27002, and adding more controls around regulated data. Do your best to define your information security program independent of legislation, but allow for legislation to shape only the areas with which it governs.

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, 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