# The Forward Looking Future

By Branden R. Williams – ISSA member, North Texas, USA chapter

Kids, gather around ol' Grandpa and let me tell you about how security was a long time ago. It used to be that we waited for a breach to happen before management got serious about security. We used to call it "getting religion." Heck, I remember working during a time when the administrative passwords were written on white boards in offices.

Pay attention, Tommy. This is important. I don't have a problem zapping you again with the attention-span ray (because in the future, you see, we replaced Ritalin with Tasers).

Now, back in the old days when Joe in Marketing would tell us on a Friday that his new product line was hitting the stores on Monday, we used to scramble to get his infrastructure ready to support it. Security was not usually considered strategic or proactive, and we were reduced to a loosely strung together series of tactical reactions. We reacted to new product lines, new attack styles, and new vulnerabilities. Ahh, yes, Super Tuesday was a big day around the office… but not as big as the quarterly Oracle release.

What's Oracle, you say? Well kids, what's left of it is that little box in the kitchen in which your Grandma stores her famous holiday recipes.

You see, in the early Twenty-First Century we didn't have fancy adaptive controls, and we laughed at the Mainframe guys with their mandatory access controls and centralized computing methods. Security was often viewed as a technical solution to a technical problem as opposed to a strategic business initiative.

Breaches in the old days were costly and frequent. It seemed like no year could pass without at least one high profile breach. Sure, we had security requirements like we do today, but they were either elementary or poorly implemented. Constituents of the free markets cried foul and begged the government to help. The first attempts were meager at best, or only applied to governments and their contractors. Even then, the adoption and maintenance of the controls was sparse and slipshod. The government eventually figured out how to create legislation that required appropriate controls derived from a basic risk model, but that took many years.

When we were the United States of America (as opposed to now being called New Tasmania…. We didn't see that coming either), both the individual states and the federal government created laws around data security. Those laws would tie irresponsible companies up in litigation from class-action lawsuits or recently elected State Attorneys-General trying to stroke the annals of history in their ink.

Shortly after Wil Wheaton[1] was elected president in the mid 2020s, all networking became ubiquitous and free. Our IPv6 devices communicated at will over the airwaves. We had to throw away our old networking models and re-think security. The light bulb finally went off, and we began making and embedding reliable and intelligent adaptive security products.

Then we harnessed quantum computing, and data protection problems became a thing of the past. Can you believe we used to think that 128-bit keys were infeasible to break? Ahh, a simpler time, when a Petabyte of storage filled a whole computer cabinet and when this thing called the iPhone was really hot technology.[2]

Within a few years of that fancy iPhone thing, consumers started holding corporations accountable for their actions with personal data. The corporations that survived in the best shape were the ones that took a strategic approach to security and stopped spending all their time putting out fires.

Savvy security professionals got a jump start on the security revolution by creating a sound strategy around security – so much so that it became a competitive differentiator. Consumer knowledge and global competition increased such that any sort of data compromise would put a measurable dent into the revenue of the company responsible.

The transition to strategic security initiatives was painful. The doers just wanted to continue pointing the fire hose at the first sight of smoke (or in some companies, the big tire fire). As with most problems, it got worse before it got better. Those companies that were brave enough to take the challenge stand strong today, so for those of you in the past that might be reading this (weird), time to step up to the challenge! Security is strategic!

## About the Author

*Branden R. Williams, CISSP, CISM is the Director of the PCI Consulting Practice at VeriSign and regularly consults with top global retailers, financial institutions, and multinationals. He can be reached at bwilliams@verisign.com or at http://www.brandenwilliams.com.*

1 http://wilwheaton.net.

2 P.S., Steve, feel free to send me one.