Herding Cats:
The Carl Method to Security

August 2008

BrandenWilliams
SECURE BUSINESS GROWTH

Before we get into this month's topic, I'd like to draw your attention to my new mugshot. The previous picture was a bit old (only a couple of years), and many of my co-workers likened it to a gopher sticking his head up out of the ground. I thought it was quite appropriate for the cube-farms that you can find in most American companies (or as I like to call them, Prairie Dog Land).

I wanted to call your attention to the old "gopher picture" not because my vanity consumes my thoughts (it only partially intrudes), but because I'd like to draw an analogy about defending the network to a classic movie. No, we're not dusting off Casablanca or The Wizard of Oz; though sometimes we all feel like hopping on a plane to get away from the flying corporate monkeys.

I want you to think about a gopher problem on a golf course maintained by groundskeeper Carl Spackler. You know, the guy that will receive total consciousness on his death bed. Among other things, he's got that going for him, which is nice.

Carl has a gopher problem. This pesky gopher dug a massive network of tunnels throughout the golf course, causing havoc. Let's let this gopher (that digs Kenny Loggins apparently) be analogous to a bad guy inside your network. In our case, the actual threat could be inside the company (a disgruntled employee) or outside (a true external threat). What do we do when we see the criminal's tunnels inside our network?

Well, if you are Carl, you try high pressure water, sniper rifles, and ultimately sculpt animal statues out of plastic explosives and weave a web of detonating wire back to a master switch. You mutter something about not minding Mr. Squirrel, manage to utter a "Fore!" and then ignite all of the explosive effigies. Normally, this would take care of the gopher (though this particular one outsmarts our groundskeeper this time as he did before). After the inferno, we see Carl leave the course a blazing mess.

CIOs are guilty of being Carl when it comes to securing and defending the network. Security spending is marginalized and de-prioritized to make room for new, dancing electronic efficiency widgets. But when neglected systems are breached, our version of "Carl" blows up the company looking for a security problem that should never have materialized.

Unlike some problems, you cannot turn the money faucet from drip to blast to make a weak security posture go away. If proper planning has not been done, security organizations will limp along for months until they get a structure in place that supports the enterprise. Not until CISOs are elevated to the board level do things start getting accomplished in a manner that matches the risk posture of the enterprise.

This is not necessarily the CIOs fault. CIOs do not really know what to do with security. Why? Because their job is different. But since they know something about that network of tubes that we call the Internet, they get stuck with security. Corporations tend to turn a blind eye to information security simply because they do not understand it. I've seen many post-breach companies that cannot believe they ignored the risk associated with a lack of strategic security for so long.

It's like a termite infestation. You do not notice the damage until your chair falls backwards at poker night, goes clear through a wall, spilling beer all over myself.

My experience with Fortune 1000 companies tells me that most have become more risk averse in the last several years. Additional legal language and reduced risk models contradict the weak security posture that is blessed by apathetic executive boards.

We learn early in our careers that absolute security is not achievable. The trick is achieving a balance between security and functionality that is palatable to the business and the budget. The business must be able to understand and accept the risk associated with what they are doing, and budgets should be adjusted accordingly to reduce the risk with product redesigns or security spending. Hopefully, then you can prevent a Carl situation from happening where the only solution is to bring in the plastic explosives.

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

<u>About the Author:</u>

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