Herding Cats:
Spread the Disease

April 2010

BRANDENWILLIAMS
SECURE BUSINESS GROWTH

Do information security professionals suffer from a form of psychosis based on the mindset required to work in information security?

The New Oxford American Dictionary, 2nd Ed. defines psychosis as “a severe mental disorder in which thought and emotions are so impaired that contact is lost with external reality.” When the regular world looks at many information security professionals, black or white hat, do you think they view our profession as a disorder?

As a developer, I was the absolute worst tester of my own applications. I always assumed that when users were presented with a screen requiring input, they would only enter the exact input in the format required . I never understood why someone would put a letter into a telephone number field, or even worse, why someone would put single quotes into search or login fields. That is, until someone demonstrated to me some pretty fancy input validation bugs that led to injected SQL statements.

I like to live my life efficiently, but I quickly realized that I had to build more tools to validate input before blindly accepting it. It’s one of those epiphany moments developers have when they go from “this input is formatted incorrectly and my reports are all garbage now,” to “Oh no, someone broke into my application and stole customer data.”

By the time I had this epiphany, I had already been bitten by the security bug working as a system administrator for a local internet service provider. I lived in the UNIX world and handled Sendmail and uw-imap vulnerabilities first hand. Since I already had some of the disease we call information security embedded into my brain, I figured out how to build my applications more securely.

I’m going into this backstory to really get to the critical question surrounding our psychosis—is it contagious? Do you have to have a genetic disposition to understand information security, or can it be a learned behavior?

I’ve been in consulting organizations big and small for the better part of a decade. One thing I’ve learned is that certain types of knowledge can be taught, and certain kinds have to be experienced. Information security is definitely one of the latter. Part of managing consultants is providing a career path and growing your talent pool in something like a pyramid[1]. In building pyramids in the past (or inheriting teams that want to cross train), it’s clear that some people get it and some people don’t.

If you want to have your own personal experience doing this, go find a family member that is not a security professional and ask her what she would do to get around a locked household door. Give her a couple of minutes to come up with some answers, and see how many she can produce. My guess is that it will be limited to things like kicking in the door or picking the lock. As security professionals, we know that there are a myriad of possibilities such as social engineering, ladders, breaking windows, using a bump key, a rig of sturdy wire, or electronic trickery that could potentially open that door. Sure, we have the experience and have seen stuff like this, but I think this psychosis causes security professionals to challenge accepted controls to find ways around them.

So back to our question, maybe it is more appropriate to ask, “Do people without a security mindset have a psychosis of some sort?” Psychosis is one of those terms that relies on social norms to define it. If the social norm is all humans were wired to be

FOOTNOTES

[1] *You want to have more smart and capable junior guys than you have super senior guys.*

terrified of any eight legged arachnid, then people unafraid of big giant spiders might be diagnosed with psychosis.

Information security professionals are absolutely rooted in external reality—our jobs depend on it. The bad guys have built a substantial business based on careless security controls. That is our external reality. Security professionals are tuned to this reality, and this alone allows us to function.

Our social norms are shifting. Not only are more people integrating technology into their daily lives, but more of us are victims of identity theft every single day. The information security mindset may be a psychosis, but I'm thankful I have it. It's one disease that is worth sharing.

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, buy his book, or reach him directly at http://www.brandenwilliams.com/.