Herding Cats:
Back to Basics

July 2010

BrandenWilliams
SECURE BUSINESS GROWTH

Like Ina Garten shows us in the kitchen, we sometimes need to stop what we are doing and get back to basics. Of course, our trade doesn't include *nearly* as much butter[1], but there are benefits to pausing our chaotic jobs to ask one simple question:

What am I trying to protect?

Many of you know me from my work in the PCI DSS space. While PCI DSS is something the industry loves to hate, many of us have used it to improve information security inside organizations. Sure, some are quick to point out weaknesses in the standard such as unauthenticated quarterly scanning and wireless security, but overall it's hard to say that PCI DSS did not contribute to securing the enterprise. Default passwords are often used as an attack vector, so it's easy to see that PCI DSS has done SOME good[2].

Unfortunately, many organizations have neglected information security so long in the name of progress and speed to market, that PCI DSS has proven to be incredibly disruptive for many companies. Compliance is the stick that is used when other methods prove to be ineffective. So if we had to go back to some basic axioms to live our information security lives by, what would they be?

Trust No Network: In this day and age, it absolutely baffles me that people still think their distributed network has never been compromised, or can be implicitly trusted. If your company sells direct to consumers and has branches or stores with computer systems, I'm talking to YOU. How can you possibly believe that your store's systems room, that probably has a false ceiling in it, would be as secure as your corporate data center? If you don't segment your networks or add in extra security features to your store networks, that's exactly what you are doing. If I can walk into your location, plug in, and be on the network, that's a problem.

Trust No Device: Expanding on the network issues above, would my personal laptop be given an IP address if I plugged it in to your network? My guess is "Absolutely!" unless you have some very specific controls around your wired network. This probably means that not only can you not trust your internal network, but you probably should not put any trust in any user-facing device on your network. That includes VoIP phones, laptops, Wi-Fi PDAs or other handheld devices, and smart phones.

Find Your Data and Defend It to the Death: Information security is all about protecting information and the assets on which it lives. You simply cannot be an effective information security professional without being absolutely sure where all of your critical data exists. The first time you go through this exercise, you will be overwhelmed. You need to first classify your data, then deploy tools or processes to go out and search for the types of data you define, and take action where appropriate (or alerting and forcing manual follow-up where it's not). Once you know where your data is, securely erase anything that is not required to do business (like employee or customer data on laptops), centralize what you need to protect and defend it to the death!

Look Over Your Shoulder: I was speaking to someone who works for a major airline the other day, and he was telling me how on his last flight he was editing a presentation for said airline outlining some of the security deficiencies he found. Somewhat normal right? What if you are flying on an airplane from that airline while editing that document? How

FOOTNOTES

[1] *If you would like to collect my man card after this bit, let me know.*

[2] *Requirement 2.1 if you are following along.*

about doing it while sitting in dead center in coach in a middle seat? How about if you are doing all of that without a privacy screen? Pay attention to what is on your screen and who is around you at all times.

If you took these four basic information security ingredients and folded them together with a cup of governance, a dash of risk management, and a few tools, what would your information security cake look like[3]? Remember, above all else, we must succeed at our jobs while keeping the business running. That means that whatever you mix together has to be edible for the business.

FOOTNOTES

[3] *Seriously, man card up for grabs.*

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