Herding Cats:
The Softer Side of Security

September 2008

Security gets a bad rap. We are often seen as an impediment to progress, a roadblock to growth, and sometimes even a black hole. If that is not bad enough, then we have the security audit.

What a way to punctuate that questionable situation with an exclamation point.

We have a responsibility to our customers, shareholders, and fellow employees to keep the bad guys out. None of us want's to be associated with a major breach. I imagine the employees of companies that suffer a significant breach do everything they can to disassociate themselves from the event that happened on their watch.

To avoid that painful situation, we often resort to auditing. I'd like to present a few tips you can use to be more successful in changing your company's security posture so you can keep their name prominently displayed on your resume down the road.

Tip 1: Assess, don't audit! People are tired of hearing the word audit. People hide things from auditors. Auditors are feared. Audit is one of the few groups that has less fans than we do. Start off by avoiding the word 'audit' at all costs. An assessment has the same end goal, but has a gentler connotation than audit does.

Tip 2: Partner, don't judge! Ok, hold on. Before we all sit around the campfire singing Kumbaya eating smores, I realize I am asking you to do something that sounds strange.

Consider how social engineering (people hacking) works. The victim who gives out the information never suspects that the person they are talking to will do something bad with it! So instead of looking down at the group you are assessing, partner with them and figure out how you can help them do their job securely. You will be shocked what you find out, so don't punish the people for opening up to you.

Tips 1 & 2 are two different ways to remind you that being successful in security depends on your attitude. The days of the IT Pedestal Warmer are gone. We will continue to be a dysfunction-inducing group until we work together with the business. Ditch the white gloves and focus on building a relationship with your co-workers—it will pay off in spades.

Tip 3: Look at the facts, but consider the risk! Before you pick up the phone and call me on this (you know who you are), realize that a security team's assessment has much more flexibility than a compliance assessment (or audit in some cases) against a particular security standard. Published policies and standards inside your company should serve as a framework that risk can be compared to.

When working with an internal customer turns up a nasty finding like that Access database that has massive amounts of customer data for 'research purposes only'—educate them. Show them that they can still have this data, but they need to spend some security dollars to protect it. Then the business owner is forced to make a business decision on that data. If the overall risk to the company is very minimal (be realistic), then consider letting it go in the short term. Be sure to document and get upper level buy off on the risk.

Tip 4: Treat first, then immunize! I am constantly amazed at the number of security professionals I see in the field that only have a tactical focus. They spend all of their time putting out fires and never actually dig deep enough to prevent the fires from happening in the first place. When you are looking at tactical findings from an assessment, don't treat it as a one off; find a way to make sure the problem will never show up in an

BrandenWrites

assessment again.

Use Tips 3 & 4 to become an enabler of secure business. We don't want to spend the rest of our lives pushing patches to the enterprise, and then hand patching the ten servers that never seem to get it on the first try. This will go a long way to becoming more strategic and less tactical in our job functions.

Strategy is vital to a company and is not easily outsourced! So go forth and partner with your internal customers and become an enabler (the good kind)!

Brandenwrites

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 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