Herding Cats:
Build Security In

October 2011

BrandenWilliams
SECURE BUSINESS GROWTH

IT has a bolt-on mentality.

I don't want that to come across as a totally negative trait as it's part of an IT person's charm. Just take a look at complex business processes implemented in IT systems and ask yourself how many components are required to make it work? And not just machines, but software like applications, operating systems, middleware, and databases. It's not just one thing—it's lots of things. And they are all bolted on with each component doing its own thing as a cog in the giant IT machine. It's how innovation in IT works. Think of all of the apps on your mobile device. All bolted on to the underlying operating system which is bolted on to the hardware which contains hundreds or thousands of electronic components (some microscopic) to make Words with Friends a pleasurable way to pass the time when I'm stuck in an airport.

So it shouldn't surprise you that security is also one of those bolted-on components into most IT systems. Very few have security built-in[1], and the ones that do sometimes miss key parts of the attack surface. It's not all their fault; imagine trying to create a foolproof system for protecting your house. Build a wall and the bad guys go around it, add an alarm system and they snip the telephone wires and power cabling, or add an extra lock and they pick it. I liken it to a developer designing fields in an application to capture a specific type of data like a US zip code. Why would someone put something in that field that doesn't meet the standard I have created?

Because most of us forget about failing safely.

Cloud and virtualization adoption is accelerating even in spite of security people screaming about the problems associated with hastily deployed IT systems. Cloud technology can be deployed securely, but managers have to understand the implications of moving information to the cloud to understand the true cost/benefit associated with the move. Cloud vendors attract customers by showing the cost savings associated with replacing traditional infrastructure. The real trick is knowing what you get with that replaced infrastructure, and how the provider bolts on security.

Yep, that's right. For the most part, they bolt it on as opposed to build it in. One easy way to tell if it is bolted on is to look at the proposal or invoice. Is there a line item for security? If so, let's hope that bolt isn't cross-threaded.

For most businesses that deal in information with value, that simply isn't acceptable. If I have compliance requirements like PCI DSS or handle healthcare data, I need security built-in to my cloud. Not only do I have lawyers expecting me to stay inside the lines, but my auditors and assessors have to see evidence that I'm staying inside the lines. The "Don't worry, we got this." attitude simply won't work for most businesses looking to move key systems into virtual- or cloud-based infrastructures with the expectation of pushing cost out of the infrastructure.

Businesses are always looking for ways to reduce their operating expenses, and IT tends to be a pretty large one these days. All companies have two levers at their disposal that they can manipulate to boost their company's performance[2]. This is why we need cloud providers to re-assess how they provide services to their customers and work to build security into their offers as opposed to bolting it on later. The cost savings to an end

FOOTNOTES

[1] *When considering the entire ecosystem.*

[2] *The other being driving revenue.*

customer aren't as great when the cloud must be secured, but that's should be expected. A feature poor security environment doesn't cost as much to operate as a security rich one.

Security managers must find ways to build relationships with the business (and not just show up when it's time to audit) such that collectively we can remove risk from our operations at the same time we are boosting the value of IT. When is the last time you had lunch with one of the business owners to understand in detail how the business operates and what their concerns are?

Many of us are finding that these very conversations help prove our own value, and begin to open doors that light a path to the boardroom.

About the Author:

Branden R. Williams, CISSP, CISM, 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 the 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