Herding Cats:
Mobile & BYOD

August 2012

BrandenWilliams
SECURE BUSINESS GROWTH

I love it when this topic comes up, which now seems to happen at least weekly. I will run into a customer or colleague that is either wading farther into the Bring Your Own Device (BYOD) waters, moving more applications to mobile platforms, or just dealing with the "IT re-prioritization machine," also known as the loudest, most senior executive who wants his new mobile device connected into the corporate network. I've even recently had a troll from a prominent technology company who couldn't believe I worked for a security company after learning about my stance on BYOD (I'm for it). The reality is that our world is shifting into a consumer-driven IT model where we directly control less data, fewer devices, and virtually none of the infrastructure that powers our business. Using traditional security methods in this reality will guarantee breaches over time.

BYOD is a good thing for businesses and information security. Yes, it's a GOOD thing. BYOD could even be the killer of legacy systems with arcane requirements and no upgrade paths . Does BYOD present a whole mess of challenges we have never faced? Certainly, but when you look at the changes you make in your controls, shouldn't those have already been there BEFORE BYOD became a thing?

Yes, they should have.

BYOD allows us to finally face the IT and infosec landscape that really began shaping up when the first laptops entered the workforce. Add a dash of remote access and the problem accelerated nearly out of control. Sure, we made a few changes here and there, but I've never met an infosec manager whose problems included too much budget and too many resources. Information security plays catch-up with the business, and many folks I have worked with have no visibility into the problems of today and tomorrow.

The basic tenets of mobile security haven't really changed over the last five years, but what has changed is the size and power of the devices coupled with the massive amount of information they can collect at any given time. So what are these basic tenets, and how do we modify them for new devices?

First, before you can even consider the device, you have to consider the data. Where does it live? How does the business consume it? Where does the business get the data, and how does it dispose of the data? How do the employees (as separated from the business systems) acquire, consume, and dispose of the data? What is the minimum view that every role in the organization needs (for sensitive data)? What security features can we wrap around the data itself? How does that work with tomorrow's IT where we don't directly control the infrastructure or the device?

Next, you have to look at the device, but in a somewhat neutral way. Every device will have a browser, and every device will have some way to install and use applications. But before you go nuts writing a bunch of code for one platform, you need to understand how your employees will procure and prefer certain devices. If you know that 80% of your population is iOS and 20% is Andriod (or vice versa), then ensure you take that into account when you are developing the app for your own corporate app store. Working to the lowest common denominator for many applications (the browser) may be sufficient for your particular application.

FOOTNOTES

[1] *In fact, even our workforce! While we push IT systems to the cloud, workers are moving the same way. Accept input, generate output.*

[2] *Do any of you still have internal applications that still require IE6?*

Finally, understand how the device and application work together with the data. Does the application store data locally? Does it wholly rely on the cloud for logic and processing? What about “offline mode”? Can you learn interesting things if you combine other phone information with the application information (like GPS to track where people go)? Did you take into account network-layer protections since you don’t control that layer?

Once you go through this exercise (and include policy, privacy, and legal reviews) you should know exactly what steps you must take in order to take advantage of this trend, which investments you will make from an infrastructure and security perspective, and how your applications will be built based on the up-front requirements. BYOD is good, and just like security professionals used compliance to build their programs in the past, we have a great opportunity to leverage BYOD to do the very same thing.

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 speaker 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