IoT Legislation

By Branden R. Williams – ISSA Distinguished Fellow, North Texas Chapter

The Internet of Things, or IoT, is more of a common term today than it was even three years ago. Google Trends shows both as increasingly popular search terms, especially in the last two years. It seems like nearly every new product has some interconnected capability, be it Wi-Fi, Bluetooth, Zigbee, or some other cool stuff that might be on the horizon. As we saw in the last half of 2016, the sheer volume of devices that are connected to the Internet can generate tremendous amounts of traffic, even though it may be powered by a relatively weak processor when compared to a computer or smartphone.

For this month, I want to talk about legislation and IoT. I believe legislation of these devices can be a good thing if it's written in the right way. That said, uninformed lawmakers tend to make a mess of technical legislation, so we should proceed with caution.

Let's examine some market pressures for a moment. I had a friend of mine come to me a couple of years ago and ask me what I thought about starting an IoT Security Consulting business. As much as I loved the idea, I asked him one question that essentially shut the whole thing down.

"Who is going to pay for it?"

When you start a business, you need to have people willing to pay you for the resources you control. In the case of consulting, it's knowledge workers and their skills. Who is the actual customer?

It's certainly not the buyer of an IoT device. Can you imagine one of us out there paying a firm thousands of dollars to evaluate an IoT device to get a report with lots of findings and then saying "Now what?" The end report would not be of much value to us as we would have as hard a time as the consumer getting the manufacturer to change things.

Can you imagine FitBit trying to communicate to the market that their pedometers are better because they couldn't be used in a botnet?

It's also not the manufacturer, even though it should be. They are rushing products to market and focusing on functionality. Unless someone is forcing the manufacturer of an IoT device to run certain checks against it, there isn't really a huge value to it. Can you imagine FitBit trying to communicate to the market that their pedometers are better because they couldn't be used in a botnet? "Like, whatever man!"

What about a distributor or seller? Again, not really much motivation there as they will only be responsible for refunds for a short period of time after the purchase of the device. Plus, they didn't make the thing in the first place.

So we're in a situation where real economic damage can be caused by a poorly built popular device and the only negative consequences would be tied back to the individuals who take them over and launch an attack. As the Mirai botnet showed us, the whole thing is a powder keg waiting to explode.

I believe nations of the developed world must take an active part in building basic guidelines for IoT devices. Since many of them require a blessing from the FCC to be mass produced, that may be the right enforcement body for products that will be sold in the US. Non-US countries have similar entities that could be leveraged in similar ways. The main tenets of the requirements would be something like 1) having a security assessment performed against it by a qualified body,[1] 2) software updates must go through similar assessments before they can go live, 3) the devices must have the ability to be updated if they connect to a network, and 4) a provision to continue to update the device in the case that the company responsible for creating it goes belly up. I'm sure there are more basic tenets like this that we could include, and I encourage you to tweet me at @ BrandenWilliams with your ideas!

Legislation is not the only way to solve the problem of poorly built IoT devices, but it certainly can be a good one. With base-level guidelines, there would be no impediment to innovation—usually the first argument against legislation of these devices. It's not an easy problem to solve, but it is a problem worth solving. It's our responsibility to do what we can to prevent further Mirai variants from shutting down commerce across the globe.

About the Author

Branden R. Williams, DBA, CISSP, CISM, is a seasoned infosec and payments executive, ISSA Distinguished Fellow, and regularly assists top global firms with their information security and technology initiatives. Read his blog, buy his books, or reach him directly at http://www.brandenwilliams.com/.

[1] Yes, I know I am opening a can of worms there. We see how poorly it's working in the PCI space, but we can learn from their mistakes.