IoT in Government: A Double-Edged Sword?

By Barry Barlow

An irreversible technological shift has occurred. We now live in a world where there is a population of seven billion people, connected to five billion devices. By the end of 2016, 6.4 billion connected units will be in use and this number is expected to grow to 11.4 billion units by 2018. But what does all this connectivity really mean, or for that fact, how will the connectivity impact our lives, our businesses, or our government?

The government, in the era of smart everything, needs to explore how it can take advantage of the increased connectivity being driven by Internet of Things (IoT). For example, identifying new citizen services and military applications that can be developed to provide tangible outcomes to constituents across the country and soldiers abroad. Or, ways for IoT to drive cost savings, increased productivity and streamlined operations. However, this shift, while opening many doors and possibilities for a better government, also represents an unprecedented change in how we view and mitigate cyber risks. As we create a more connected world, we also expand the attack surface for cyber criminals and expose new vulnerabilities in our networks.

Government agencies are adopting IoT best practices as a means to move their missions forward. Take the Department of Defense (DoD) for example. As with most technology and innovation, the DoD is leading the way and operating at the cutting edge. The DoD launched an integrated fighting system program for U.S. infantry soldiers, long before similar solutions in the commercial sector started popping up. This program replaces the traditional joint task force model of today and allows soldiers to closely coordinate and share up-to-date battle statuses to command centers back home. Truly every soldier is a sensor on the modern battlefield.

On the civilian side of government, the United States Department of Agriculture (USDA) uses tablets to allow the department's field agents to log information whenever and wherever they have an Internet connection. And in healthcare, hospitals all over the nation are using IoT to store and share valuable data, and even take action (e.g., change the desired temperature in a patient's room). These applications are just a few examples of the types of operations that government agencies should adopt to take advantage of the increased connectivity.

In the commercial sector, the demand for increased mobility is one of the biggest drivers behind the adoption of IoT. Mobile devices are, without question, the largest component of IoT today and account for 60 percent of all connected devices. However, currently, neither businesses nor the government is prepared to handle the massive influx of data that will come with the all of the new mobile services. Both parties must invest to ensure the security of data, and in smart data analytics tools to translate all of the new data sets that will start flooding the IT infrastructure.

It is not possible to truly reap the benefits of IoT without being able to make sense of the huge number of data sets. In this day and age, connectivity requires analysis. IoT analytics are critical. In one final example, over 100 cities across the world in places like Dallas, Chicago, Barcelona, Dubai and elsewhere are moving forward in an IoT concept known as "connected cities." More than just offering Wi-Fi hotspots in public places, connected cities also include connected traffic management systems, public transportation, lighting management, environmental monitoring, public safety and security systems all connected to an operations center. Via location-based data, the city planners know where people are, what (and how) they are driving, what services are being used and can take action accordingly.

We have the potential to change federal government operations to create a better, smarter, more user friendly government – while still ensuring security. It is in the government's best interest to help strike a balance between assuming new risk from cyber threats and unlocking the potential benefits of IoT for the American public.

Barry Barlow is the Senior Vice President and Chief Technology Officer at Vencore, Inc. In this role, he ensures Vencore is positioned for short- and long-term success by assessing the technology needs of our customers, partners and suppliers, as well as developing a corporate technology roadmap to meet those needs

VENCORE®

15052 CONFERENCE CENTER DRIVE | CHANTILLY, VA 20151
TEL: (571) 313-6000 | VENCORE.COM