Letter from the Editor

By: Scott St. John

A revolution is surging. An army comprised of billions of devices is advancing and beating against the castle walls of even the largest service providers. If the industry is not prepared for the onslaught of the Internet of Things (IoT) it will have disastrous consequences. But it's not all doom and gloom, as there is an opportunity to prepare for, and even win, this war.

What does this army look like? Chances are if you are reading this article you are wearing one on your arm right now — with 200+ million wearable devices hitting the market this year — a number that is projected to more than double by 2022. But it's much more than just smart watches and Fitbits. Every "thing" is becoming increasingly connected from your car to your home to your city. At the same time, enterprises, factories, and even entire industries are being transformed by the IoT. And yes, that includes robots.

But let's not gloss over the aforementioned disastrous consequences. In 2016, DNS provider Dyn was attacked using the Mirai botnet malware, taking out most of the connectivity across the Easter coast of the United States and hundreds of thousands of websites, including commercial sites such as Amazon, Paypal and Visa. The attack was conducted by turning millions of connected devices, such as video cameras and DVRs, into malicious agents that overwhelmed Dyn's network. The damage estimates are nearly incalculable. For Dyn, over 140,000 customers immediately stopped using their service. For the damages to the thousands of commercial businesses that relied on Dyn's services, estimates range between $1 and $1000 *per minute*. And, if you think the Dyn story is too played out, just last month the city of Riviera Beach, Florida announced it was going to pay over a half a million dollars to hackers who seized its computer systems as a result of a ransomware attack. Which is why we dedicated two articles this month to the topic of IoT Security, and it is a prevent theme in several others.

In this issue of *Pipeline*, we hear from Dr. Mark Cummings and Bill Yeack about the security risk and opportunity for the IoT. We also explore four key strategies for network security and IoT innovation with Masergy. We gain perspective with Ericsson on the eight dimensions of IoT and look at methodologies for realizing the IoT opportunity with Nectar Services. We also take a look at the device revolution with InfiNet Wireless, who is helping to make smart cities a reality in Brazil; and from the WiMAX Forum on how they are helping standardize airport surface communications. We explore the fiber imperative for IoT with Clearfield and how AI is transforming the enterprise and data centers with eStruxture Data Centers. We also look at managing the evolution of the SIM lifecycle with Evolving Systems, take a look back at the month's news in our monthly industry news column, and much more.

We hope you enjoy this and every issue of *Pipeline*,

Scott St. John
Managing Editor
Pipeline