IoT innovation in India

Posted by Andrew_Moore in IT Peer Network on 25-Feb-2015 10:37:22

If there's one thing that sums up the spirit of India, it is this:

A man weaving between cars in slow-moving traffic — selling sun visors, peanuts, and of course, the *Harvard Business Review.*

I saw this on my recent trip to Mumbai and Delhi, where I was running two CIO Executive Forums. At these events, I noticed the same street-savvy, entrepreneurial flair within business and tech leaders at the board level. Executives from across the political spectrum were uniting behind the government's agenda for change.

Both events were well attended, and the conversation focused on the major trends driving the need for IT transformation across various industries. Through these conversations, I was struck with the realization that the time gap between technologies arising in mature markets and becoming a reality in emerging markets is ever shrinking.

IoT Innovation

One of the hottest areas for reinventing businesses today is on the topic of the Internet of Things (IoT). There was a lot of discussion around the subject with a clear understanding that change and rapid innovation are critical for success. One financial services CEO said: "For us to succeed and lead the market, it's imperative that we keep reinventing ourselves."

Some attendees were still looking for the right business applications for IoT, or researching how to put it into action. However, I was surprised by the number of executives who were already deploying live applications or engaging in trials.

IoT Security

Within the realm of IoT, another top priority for everyone was security. We've already seen headlines about fridges and other domestic devices being hacked, and there's rarely a day that passes without another headline report about the latest large scale attack — often with a "connected device" as the entry point. As the number of smart devices grows, so does the number of potential attacks on them. Many estimates on the total number of connected devices hover around 50Bn by 2020. In 2015, the manufacturing, utilities and transportation sectors will have 736 million connected devices based on Gartner estimates — all of which must be protected against misuse.

 The vast number of connected things presents a challenge. But so too does the breadth of technologies involved. The point of attack can now span across a number of technology layers – including edge devices, communications networks, and the cloud. All of these layers must be protected against intrusion and abuse. Many of the advantages of the Internet of Things disappear if security is managed on an individual device basis. A scalable secure solution is a crucial and fundamental need. One way to achieve this is to use a single security policy management solution to manage the device, software and data security in the IoT gateway solution. To support this strategy, this same solution can be used for managing the IT infrastructure. This approach enables security across the IT and IoT infrastructure to be monitored and managed through a single interface — reducing the complexity of protecting a dispersed and technologically diverse network of devices, and making the security management scalable as the data gathering.

IoT Privacy

Privacy was another mentioned priority for IoT. A robust privacy safeguard will be essential to win the trust of the owners of connected devices. Applications that deliver benefits to end users often have the side effect of exposing potentially private information to a service provider. One way around that is to use anonymity features at the processor level that enable service providers to address groups of users without knowing the identity of each one. For example, a group of cars might be authorized to use specific transport information services while the provider would deliver these services without identifying individual cars and their drivers. Intel is working with other silicon manufacturers to implement this concept, to ensure that hardware-based privacy can become a standard component of IoT.

IoT Agility

One final and more general observation was around agility. It was clear from the interactions with customers that they recognize the need to innovate quickly. To stay ahead, solution deployments should be scheduled in days and weeks rather than months and years. While this kind of timeframe was previously unheard of, a foundational step towards this agility is to deploy modern infrastructure.

All in all, my experience in India was fantastic. It was a truly insightful meeting of minds on the subject on the Internet of Things. Seeing the innovation coming out of this region was exciting and I look forward to the ever-developing technology of IoT.

Find out more about how Intel can help you to implement the Internet of Things

-Andrew Moore