The Internet of Things in 2018: predictions, problems, possibilities

Insight Guide

2017: A Dynamic Year

2017 was a dynamic year for the Internet of Things. Over those 12 months, we watched much of the early hype around connected technology and its enterprise applications become a dynamic reality. Tangible use cases of the IoT proliferated across a range of diverse sectors, from medicine to agriculture. Global companies announced new IoT strategies and offerings, including the launch of Intel's Retail Responsive Platform in January, with a $100 million investment to follow, and the beta launch of Google's Cloud IoT Core in May. In November, IWS added a number of impressive new analytics capabilities to its AWS IoT Core platform. And the year was rounded off with smart home assistants like the Google Home and the Amazon Echo being top of many must-have Christmas lists.

In a less positive light, IoT security hit the headlines throughout the year, as the vast and growing number of connected devices worldwide proved a rich hunting ground for cybercriminals. Huge DDoS attacks were attributed to poor IoT security, while as many as five billion Android, Microsoft, Linux and iOS devices were said to be exposed to a Bluetooth vulnerability.

In many ways, then, 2017 could be seen as a year in which the IoT went truly mainstream. More and more consumers are aware of the IoT beyond the realm of smart fridges and driverless cars, while more and more organisations and industries are exploring ways in which the IoT can help them drive tangible operational improvements.

What, then, do the next 12 months have in store? Here are our five key predictions.

Head in the Clouds

Plenty of organisations manage their IoT infrastructures out of on-site datacentres, and this isn't going to go away completely. However, the cloud is already an attractive choice for hosting and managing enterprise IoT ecosystems – for all the same reasons that apply to other aspects of organisational IT. The cloud makes IoT deployments faster and more elastic, reduces upfront costs, offers global scale more or less at the click of a button, and is easy to manage and maintain. It's a tempting proposition, and global corporations like Google and Amazon are clearly banking on plenty of organisations being tempted by it.

All that said, plenty of smaller, speciality players also offer cloud-based analytics engines and IoT management platforms, and we expect to see the profile of these go up and up throughout 2018.

Sector Specialisation

As with so many other technological innovations before it, as the IoT moves from experimental innovation to maturity, so too will IoT developers and manufacturers shift from broad strategies to more industry-specific ones. The early signs are already there. We've seen the emergence of the Industrial Internet of Things (IIoT), for example, whereby webs of connected sensors on factory floors are driving more proactive approaches to hardware maintenance and more efficient production lines – this, ultimately, is leading to the development of smart factories. We've watched the IoT make waves at every level of the medical sector, from consumer-focused wearables like heartrate monitors and activity trackers, through to highly sophisticated connected medical devices and IoT-enabled hospital machinery such as chemotherapy stations and pharmacy dispensers. In transport, the IoT is powering the development of connected fleets and a more proactive approach to scheduling public transport, while the utilities sector has taken the IoT far beyond smart homes and into the development of entire smart grids.

But this sector specialisation has by no means reached its peak. Throughout 2018, we expect to see the emergence of more industry-specific IoT specialisms, like the IIoT, as more and more sectors hone and strengthen their bespoke approaches to this flexible technology.

Business to Business

The Internet of Things first captured end user imagination through stories about driverless cars and fridges that would automatically restock themselves when they ran out of milk. Even now, it's the thermostats and security cameras behind so-called 'smart homes', and the rise of personal assistant devices like the Amazon Echo and the Google Home, which remain at the forefront of many people's minds when the IoT is mentioned.

Throughout 2018, we expect business-to-business applications of the IoT to gain more mainstream prominence, as more and more enterprises switch on the huge power of the data that can be collected via the IoT. We expect to see more discussion around the data that can be captured in enterprise settings via the IoT, and the business problems and challenges that can be met through innovative deployments of the IoT. Indeed, beginning discussions with a consideration of problems to be solved or business objectives to be achieved is the best way for any enterprise IoT strategy to begin.

Security Shake-ups

With the EU GDPR due to come into force in May 2018, the notion of 'privacy by design' is on everyone's lips. Of course, all savvy and forward-thinking IoT businesses have been considering the impact of this regulation – and the question of cybersecurity more generally – for some time now, but as the date rolls nearer, no business will be able to ignore it.

Meanwhile, Forrester Research has suggested that money-oriented IoT attacks are likely to increase in 2018. Rich pickings can be available for cybercriminals who successfully infect IoT ecosystems with ransomware, after all. Unfortunately, we think that this prediction will likely to be borne out. 2018 seems likely to be a year of more and more cyberattacks on both connected devices and the IoT platforms they run on – making it more important than ever for businesses developing or deploying connected products to implement good security practices from the very beginnings of their lifecycles.

While no one wants to see a huge, headline-grabbing cybercrime story traced back to an IoT vulnerability or oversight, there is every chance that this could happen in 2018. More connected devices mean, very simply, more potential targets for cybercriminals, and too many IoT designers and manufacturers are still not embedding the same robust security protocols into their products that exist in other aspects of corporate IT.

Feedback Loops

On a happier note, we think that product designers, as well as marketing and even sales personnel, are poised to take much greater advantage of the wealth of data that can be generated by IoT devices. The IoT can, for example, enable designers to access real, live information on how products are being used 'in the field', or to assess different manufacturing processes against each other. And with this information at their fingertips, it is possible to make lightning-fast and well-informed design alterations, test them and push them live more quickly than ever before. This 'feedback loop' structure is a key part of how IoT businesses can effectively evolve the user experience of their products – and that, in turn, is a key part of business success. We expect to see far more of it in 2018.