tern

Realising the true value of IoT

Insight Guide

A fourth industrial revolution

There is no shortage of news around the Internet of Things (IoT). Some hail it as a harbinger of the fourth industrial revolution and a new economic paradigm of connectivity and business transformation.

To others it’s the subject of cautionary tales - an unguarded back door through which hackers can take over insulin pumps, steal personal data and shut off power to entire cities.

In this guide, we cover what the reality of the industry is today, the use cases in practice and the essential enablers for the success of the IoT.

What’s the reality?

Transforming business models to create better experiences for customers, competitive advantage and operational efficiencies.

When The IoT is set to be more disruptive and far reaching than many realise. If approached correctly, it can transform entire business models and lead to unprecedented competitive advantage. It can revolutionise customer experience, streamline operations, completely alter product and service design and deliver new business models and revenue streams.

IoT is best understood not as a technology revolution, but as a business revolution that technology made possible. At its core, IoT is about using information from connected devices to help business owners and leaders make smart decisions about business.

Information fuels business. And devices help you access and use business-critical information every day. For example, it’s easy to understand the value of collecting and keeping customer information—whether you use the contact list on your smartphone or a CRM solution—because that information helps you better serve customers in the future.

Now think about all of the electronic devices you use in your business every day—not just your computers and phones, but also your equipment on the factory floor, delivery trucks, point-of-sale kiosks, cash registers and credit card processing terminals, cameras, sensors and security systems. These devices all have the potential to collect information too—from work patterns and processes to the ways people move through and interact with the environment. If you had all these devices connected and communicating with one another, imagine what kind of business possibilities you could create from the information they collect.

IoT goes one step further

It not only gives you a way to connect these devices and gather relevant information from them, but also helps you practically apply that insight.

For example, a retailer can use security cameras to see where people spend the most time in the store and which displays are generating the most interest. Combine that with the sales data from EPOS, and the retailer can make decisions about how and where to display merchandise to drive more sales.

Sensors and devices in delivery trucks can do things like monitor driver safety, fuel efficiency, and route options. Gather all that information in real time and combine it with other data such as traffic patterns, diversions, and weather forecasts, and it could influence your routing decisions, keep your drivers safer, and save the company time and money. Bottom-line value: IoT provides the connective infrastructure that lets you collect information from disparate devices, store it, visualise it, analyse it—and use it to make smart decisions.

Essential enablers of IoT

The success of IoT requires certain conditions to be in place, notably overcoming a number of hurdles technical, organisational and cultural. So, what are the essential enablers that will maximise IoT impact?

Hardware Infrastructure

One of the basic requirements of IoT is to have the capacity for millions of devices, machines, and computers to talk to each other, sometimes across large distances. For this to happen, two types of technology are needed to create the infrastructure on which the IoT can operate: cheap, low-power hardware and reliable connectivity.

- Low-cost, low-power hardware

The cost of components and computing power must continue to drop to make IoT applications cost-effective. Today many applications are technically solvable, but the high cost of components such as sensor nodes makes implementation impractical. However, the declining costs of microelectronics should make critical components more affordable. Sensor nodes not only need to be low-cost, but in many remote applications where they cannot be connected to an electrical service they will also need to consume little power.

Long-lasting batteries and local power sources can enable many IoT applications, such as monitoring remote equipment. Low-cost, low-power sensors are also needed in applications such as precision agriculture, where many sensors are necessary for monitoring soil moisture.

- Reliable connectivity

Many short-distance connections to IoT sensors don't require cellular data services because the data will travel over low-power local area networks. However, many applications that require more complex analytic computing of data from diverse sources will need alternative, cost-effective connectivity. Even at the best of times wireless data services can be patchy and unreliable outside urban areas—where many factories, warehouses, and other industrial buildings are located. Though options are available, some remain extremely expensive.

Analytics

Access to new and valuable data is at the heart of the IoT. IoT data really is Big Data. Collected from a huge number of embedded sensors, geographies, devices and the cloud, the data is unstructured, with streams of information available from an array of sources in real time.

The rapid ability to derive meaning from this data, and to quickly respond to new information is central to the promise of the IoT. For example, autonomous driving vehicles will only be viable when the data associated with each vehicle's activities can be processed and assessed so that a continuous stream of near real-time commands flow in response to the changing data received as each vehicle's trip progresses.

Even with knowledge and expertise in data analytics, all companies looking to profit from the IoT – and improve customer experience – will need to re-examine their approach to data analytics. The success of any IoT project, to drive revenue on the business side, and to provide new, better and personalised services on the consumer side, lies in a company's ability to intelligently harness and capitalise on data through advanced analytics systems that can continually process data and generate actionable information, alerts, and reports.

Currently, only one third of organisations in Europe are analysing data generated by their IoT initiatives [IoT & the Data Analytics Challenge, Telefonica 2017], meaning the majority remain ignorant to its potential, and are failing to make the most of their investments in this area. This lack of IoT data insight means consumers too are missing out.

Analytics software has not progressed to the point where it can be easily applied in every case. The hard work of developing and tuning algorithms for the peculiarities of specific use cases is largely still undone, and the skills and capabilities to do this work remain in short supply. New business models must be adopted to address this, supported by tools to assist companies in monetising data.

Interoperability

In any interconnected system, all of its component devices must be able to communicate with each other. A lack of common software interfaces, standard data formats, and common connectivity protocols creates a challenging landscape.

For industries, this means that up to 40% of the total value of the Industrial IoT will remain inaccessible because different systems cannot work together. In addition, the drive to seamless interoperability is further obstructed by the long lifespan of traditional devices that require costly retrofitting, or even replacement, to work with the latest technologies.

Bridging the gaps in communications between devices and the rest of the Internet will require middleware or gateways that ensure interoperability throughout a network by translating the data from one protocol to another. However, it is critical that, with the number of network devices and protocols quickly growing, the middleware delivers fast protocol conversion.

Security

The Internet of Things heightens existing concerns about cyber security and introduces new risks. It multiplies the normal risks associated with any data communication; each device increases the “surface area” available for breaches, and interoperability expands the potential scope of breaches.

Every node is a potential entry point, and interconnection can spread the damage. A disrupted medical monitor could pose life-and-death risks. A hacker attack on a smart grid system could potentially turn off power to millions of households and businesses, creating massive economic harm and threats to health and safety. For individuals, IoT security breaches can involve both inappropriate use of personal data and theft.

While there are many industry-specific standards and best practices that address information security, standards and best practices specific to IoT technologies are still in development or not widely adopted. Traditional cyber security has focused on perimeter defense and detection and remediation. That does not work in a world of ubiquitous IoT devices that run thousands of applications and that operate on multiple networks simultaneously.

Effective IoT security solutions must serve, at minimum, a triple purpose: first, automatically and autonomously control from the very start, which devices can connect, secondly ensure the integrity and privacy of the data generated by IoT devices and moving through IoT networks. Thirdly, through autonomous authentication and attestation ensure only authorised users can access the information thus preventing IoT devices from malicious hackers who could conceivably take unauthorised control of IoT devices and/or their applications. And all this has to be done automatically.

Redesigning new security frameworks that span the entire cyber physical stack is not negotiable for the enterprise. Businesses need to make sure that IoT devices have strong device centric identity, authentication, integrity and access controls for end-to-end data transfers.

Organisational culture

Driving IoT implementation will bring up new challenges, not least in connecting business systems across business boundaries. This needs strong company wide collaboration, championed by leadership.

No one person or department can plan and implement an IoT strategy alone – nor should they, as for IoT to live up to its potential, organisations need to join the dots between existing silos of information.

A pivotal convergence also needs to happen between the IT and OT divisions. Control engineers must up skill so that they in the very least understand networking and security and IT engineers and architects must understand the difference between business processes and manufacturing processes.

Talent

Most industrial companies don’t have the IT resources or skills to build an IoT solution internally in a way that’s cost-effective and fast..

Indeed many companies are concerned their teams lack the skills and understanding to exploit IoT and big data.

According to a research report produced by service provider Capita Technology Solutions (CTS) and networking supplier Cisco, 70% of respondents said they found it relevant to their business, but 71% said they did not have the skills to identify the growth opportunities it offered.

The true value of IoT comes in combining connected intelligence to deliver an overarching view, which will allow organisations to optimise operations, differentiate their services and enable new business models. Though challenges remain, these aren’t insurmountable and organisations are already starting to realise the benefits of the IoT, particularly in the industrial space.