

AUGUST 2015

McKinsey Quarterly

# An executive's guide to the Internet of Things

Jacques Bughin, Michael Chui, and James Manyika

The rate of adoption is accelerating. Here are six things you need to know.

**As the Internet of Things (IoT)** has gained popular attention in the five years since we first published on the topic,<sup>1</sup> it has also beguiled executives. When physical assets equipped with sensors give an information system the ability to capture, communicate, and process data—and even, in a sense, to collaborate—they create game-changing opportunities: production efficiency, distribution, and innovation all stand to benefit immensely. While the consumer's adoption of fitness bands and connected household appliances might generate more media buzz, the potential for business usage is much greater. Research from the McKinsey Global Institute suggests that the operational efficiencies and greater market reach IoT affords will create substantial value in many industries.<sup>2</sup>

There are many implications for senior leaders across this horizon of change. In what follows, we identify three sets of opportunities: expanding pools of value in global B2B markets, new levers of operational excellence, and possibilities for innovative business models. In parallel, executives will need to deal with three sets of challenges: organizational misalignment, technological interoperability and analytics hurdles, and heightened cybersecurity risks.

<sup>1</sup> See Michael Chui, Markus Löffler, and Roger Roberts, "The Internet of Things," *McKinsey Quarterly*, March 2010, [mckinsey.com](http://mckinsey.com).

<sup>2</sup> For the full McKinsey Global Institute report, see *The Internet of Things: Mapping the value beyond the hype*, June 2015, on [mckinsey.com](http://mckinsey.com). We analyzed more than 150 IoT use cases across the global economy, and using detailed bottom-up economic modeling, we estimated the economic impact of these applications across a number of dimensions.

## Opportunities beckon . . .

IoT's impact is already extending beyond its early, most visible applications. A much greater potential remains to be tapped.

### Creating B2B value globally

To make the Internet of Things more understandable, media coverage has often focused on consumer applications, such as wearable health and fitness devices, as well as the automation products that create smart homes. Our research reveals considerable value in those areas. Yet the more visible manifestations of IoT's power shouldn't distract executives from a core fact: business-to-business applications will account for nearly 70 percent of the value that we estimate will flow from IoT in the next ten years. We believe it could create as much as \$11.1 trillion a year globally in economic value in nine different types of physical settings. Nearly \$5 trillion would be generated almost exclusively in B2B settings: factories in the extended sense, such as those in manufacturing, agriculture, and even healthcare environments; work sites across mining, oil and gas, and construction; and, finally, offices.

There's also a global dimension to IoT's B2B potential. Emerging markets, whose manufacturing-intensive economies often supply goods to final manufacturers, will be prime areas for IoT adoption. But over the next ten years, the total economic impact from IoT will be greater in advanced economies, given the possibility of larger cost savings and higher adoption rates (Exhibit 1).

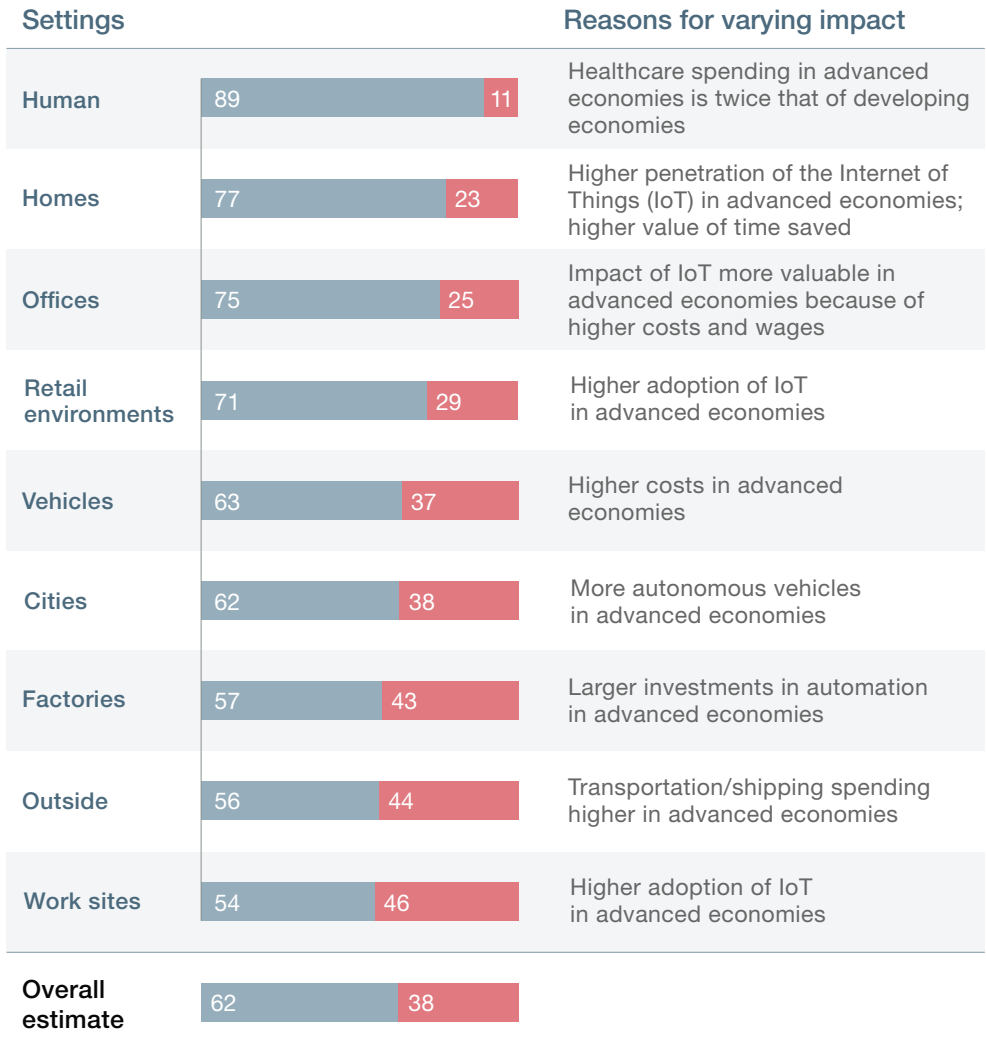
However, an estimated 38 percent of IoT's overall worldwide value will likely be generated in developing economies, and eventually, the number of IoT deployments in such markets could surpass those in developed ones. In fact, deployments in developing economies are likely to exceed the global average in work-site settings (such as mining, oil and gas drilling, and construction) and in factories. For instance, China, with its large and growing industrial and manufacturing base, stands to reap major benefits not only on the factory floor but also in product distribution. In fact, developing economies could leapfrog the developed world in some IoT applications because there are fewer legacy technologies to displace.

Exhibit 1

## The economic impact of the Internet of Things will be greater in advanced economies.

Share of economic impact, 2025, %

■ Advanced economies ■ Developing economies



## Optimizing operations

Investing in IoT hardware—from sensors embedded in manufacturing equipment and products to electronically tagged items along the supply chain—is only the starting point of the value equation. The biggest competitive gains come when IoT data inform decisions. Our work shows that most of the new business value will arise from optimizing operations. For example, in factories, sensors will make processes more efficient, providing a constant flow of data to optimize workflows and staffing:

- Sensor data that are used to predict when equipment is wearing down or needs repair can reduce maintenance costs by as much as 40 percent and cut unplanned downtime in half.
- Inventory management could change radically, as well. At auto-parts supplier Würth USA, cameras measure the number of components in iBins along production lines, and an inventory-management system automatically places supply orders to refill the containers.
- In mining, self-driving vehicles promise to raise productivity by 25 percent and output by 5 percent or more. They could also cut health and safety costs as much as 20 percent by reducing the number of workplace accidents.

IoT systems can also take the guesswork out of product development by gathering data about how products (including capital goods) function, as well as how they are actually used. Using data from equipment rather than information from customer focus groups or surveys, manufacturers will be able to modify designs so that new models perform better and to learn what features and functionality aren't used and should therefore be eliminated or redesigned. By analyzing usage data, for example, a carmaker found that customers were not using the seat heater as frequently as would be expected from weather data. That information prompted a redesign to allow easier access: the carmaker updated the software for the dashboard touchscreen to include the seat-heater command. This illustrates another capability of connected devices: with the ability to download new features, these products can actually become more robust and valuable while in service, rather than depreciate in value.

Despite this value, most data generated by existing IoT sensors are ignored. In the oil-drilling industry, an early adopter, we found that only 1 percent of the data from the 30,000 sensors on a typical oil rig are used, and even this small fraction of data is not used for optimization, prediction, and data-driven decision making, which can drive large amounts of incremental value.

### Creating innovative business models

IoT can also spur new business models that would shift competitive dynamics within industries. One example is using IoT data and connectivity to transform the sale of industrial machinery and other goods into a service. The pioneers of this trend were jet-engine manufacturers that shifted their business model to selling thrust and ancillary services rather than physical equipment. Now these models are proliferating across industries and settings. Transportation as a service, enabled by apps and geolocation devices, is encroaching on vehicle sales and traditional distribution alike. Manufacturers of products such as laser printers with IoT capabilities are morphing into robust service businesses.

IoT makes these business models possible in a number of ways. First, the ability to track when and how physical assets are actually used allows providers to price and charge for use. Second, the combined data from all these connected assets help a supplier to operate equipment much more efficiently than its customers would, since its customers would only have a limited view of their own equipment if they purchased and ran it themselves. Furthermore, analysis of IoT data can enable condition-based, predictive maintenance, which minimizes unplanned downtime.

This business-model shift will require product companies to develop and flex their service muscles. Product development, for instance, becomes service development, where value is cocreated with customers. It won't be enough to focus on the product features customers will pay the most for. Developers will need to understand the business outcomes their customers seek and learn how to shape offerings to facilitate those outcomes most effectively. Service providers will also have to take on capacity-planning functions—including planning for peak usage and utilizing IoT data to forecast demand.

## **. . . but challenges remain**

As with any major technological shift, realizing IoT's potential will require significant management attention not just to new technical imperatives but also to organizational issues.

### **Aligning the organization**

IoT will challenge traditional organizational roles as information technology becomes widely embedded across assets, inventories, and operations. One focal point will be the IT function, for the Internet of Things requires it to assume a transformed role that spans beyond computers, networks, mobile devices, and data centers. Instead, IT will have to join with line managers to oversee IoT systems that are essential to improve both the top and bottom lines.

In retailing, for instance, one of the largest sources of value could be the sales lift that real-time, in-store personalized offers are expected to deliver. This will require the sophisticated integration of data across many sources: real-time location data (the shopper's whereabouts in a store), which would link to data from sensors in the building; customer-relationship-management data, including the shopper's online-browsing history; and data from tags in the items on display, telling the customer to enter a specific aisle, where he or she could use an instant coupon sent to a phone to buy an item previously viewed online. In short, information technology and operations technology will converge, both technically and in their metrics of success. As a result, companies will have to align their IT and operational leadership tightly, though traditionally these functions tended to work separately and, more often than not, held each other at arm's length.

Beyond expanding IT's role, IoT will challenge other notions of organizational responsibilities. Chief financial, marketing, and operating officers, as well as leaders of business units, will have to be receptive to linking up their systems. Companies may need to train employees in new skills, so the organization can become more analytically rigorous and data driven. Analytics experts and data scientists must be connected with executive decision makers and (to optimize insights from the new data) with frontline managers. In some cases, the decision makers will be algorithms. When

companies need large-scale real-time action—such as optimizing the control of equipment across an entire factory—IoT systems will make decisions automatically. Managers will monitor metrics and set policy.

### Overcoming interoperability and analytics hurdles

Strategies that use IoT data in an effective way often call for interoperability. We estimate that nearly 40 percent of the potential value, on average, will require different IoT systems to communicate with one another and to integrate data (Exhibit 2). Relatively little of that is happening now. For example, on offshore oil platforms today, components such as pumps are often installed as connected devices, but in a limited fashion: devices individually connect back to their manufacturers, which monitor and control machines and can optimize their maintenance and performance individually. However, data from multiple components and systems must be combined to identify more than half of the predictable performance issues that arise in day-to-day platform operations, including those that could impact overall oil-production volumes.

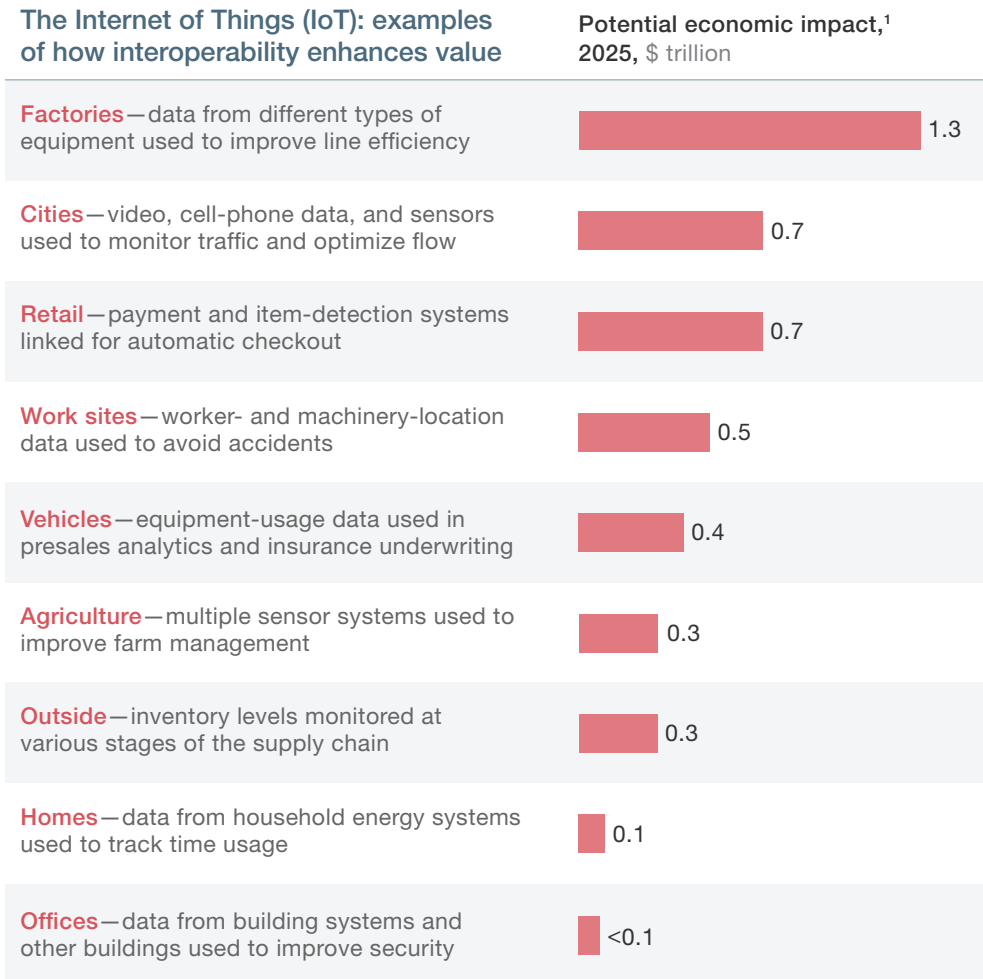
Many large companies will have enough market power to specify that their IoT vendors make systems interoperable. In some cases, this will lead vendors to choose common standards that will ultimately speed up adoption. In other cases, interoperability could also be achieved with software platforms designed to combine data from multiple systems. That will create new market opportunities for companies capable of integrating data from diverse sources.

However, simply bringing data together from different IoT systems won't be enough. Indeed, IoT may exacerbate many of the challenges we have observed when companies use big data.<sup>3</sup> In moving to a world where IoT is used for prediction and optimization, companies face an analytics challenge. They'll need to develop or purchase, to customize, and then to deploy analytical software that extracts actionable insights from the torrent of data IoT will generate. And in many cases, the algorithms embedded in this software will have to analyze data streams in real time—a task many traditional analytical tools are not designed to do. This offers another potential market opportunity for innovative software developers.

<sup>3</sup> For more, see *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, May 2011, on [mckinsey.com](http://mckinsey.com).

## Exhibit 2

## IoT's interoperability could deliver over \$4 trillion out of an \$11.1 trillion economic impact.



<sup>1</sup>Includes sized applications only; includes consumer surplus.

McKinsey&Company | Source: Expert interviews; McKinsey Global Institute analysis

### Facing up to the security imperative

The prospect of implementing the Internet of Things should prompt even greater concern about cybersecurity among executives. IoT poses not only the normal risks associated with the increased use of data but also the vastly greater risks of systemic breaches as organizations connect to millions of embedded sensors and communications devices. Each is a potential entry point for



malicious hackers, and the damage from a break-in can be literally life threatening—disrupting machine-control systems on an oil rig or in a hospital, for example. The same interoperability that creates operational efficiency and effectiveness also exposes more of a company’s units to cyberrisks. Growing interconnections among companies and links with consumer devices will create other challenges to the integrity of corporate networks, too.

Companies will need to rely on the capabilities of vendors to mitigate some of these risks. However, preparing for a revolutionary change in distributed connectedness and computation will also require a new strategic approach, which our colleagues have described as “digital resilience.”<sup>4</sup> In other words, companies need to embed methods of protecting critical information into technology architectures, business-model-innovation processes, and interactions with customers. They can start by assessing the full set of risks in an integrated way and by creating an extensive system of defenses that will be hard for hackers to penetrate. Companies also need to tailor cybersecurity protections to the processes and information assets of each of their businesses, which in an IoT world will increasingly be linked. Given the extent of the risks and the cross-functional nature (and significant cost) of the solutions, progress will require senior-level participation and input.



IoT will soon become a differentiating factor in competition. Senior leaders and board members must take a systems approach to address the organizational challenges and risks this expansion of the digital domain will create. That will allow companies to capture the full range of benefits promised by the Internet of Things. ○

<sup>4</sup> See Tucker Bailey, James M. Kaplan, and Chris Rezek, “Repelling the cyberattackers,” *McKinsey Quarterly*, July 2015, [mckinsey.com](http://mckinsey.com).

*The authors wish to thank McKinsey’s Dan Aharon and Mark Patel for their contributions to this article.*

**Jacques Bughin** is a director in McKinsey’s Brussels office; **Michael Chui** is a partner at the McKinsey Global Institute, where **James Manyika** is a director.