McKinsey&Company

NOVEMBER 2015

© Alex Belomlinsky/Getty Images

Business Technology Office

Preparing IT systems and organizations for the Internet of Things

To accommodate the development and support of smart devices, companies will need to update existing IT architectures and operating models. Here's a potential road map.

Johannes Deichmann, Matthias Roggendorf, and Dominik Wee

As the Internet of Things (IoT) gains momentum, many companies are trying to determine how best to update their existing IT architectures and operations to capitalize on this trend.

The Internet of Things refers to the networking of physical objects through the use of embedded sensors, actuators, and other devices that can collect or transmit information about the objects. Examples in the consumer market include smart watches, fitness bands, and home-security systems. Examples in the B2B market include sensor-embedded production equipment and shipping and storage containers. Such devices are networked through computer systems and generate an enormous amount of data—information that some leading-edge companies are mining for insights and opportunities that can help set them apart from competitors.

According to a recent McKinsey Global Institute report, the networking efficiencies and opportunities created by the Internet of Things may have a global economic impact of as much as $11 trillion per year by 2025 across multiple sectors.[1] The report also suggests that, although consumer applications seem to be on the leading edge of adoption, nearly 70 percent of the projected economic value will eventually come from the use of sensor technology and swarm intelligence among B2B users.[2]

Takeaways

Although there’s a huge opportunity in the Internet of Things, much uncertainty remains: many companies need to redesign their technology stacks and embrace agile software development to better serve customers, for example.

To retool and meet the challenges ahead, leaders should focus on seven principles.

A considerable advantage could be gained by those that help set technology standards, factor connectivity into design, embrace a continuous-delivery model, retrofit existing products and systems, update cybersecurity strategies, explore interoperability and open-source technology, and devise new organizational structures.

The opportunity is huge, but there is a lot of uncertainty for companies, as there is with any emerging trend. Questions remain about how to accurately assess the business opportunities in the Internet of Things, how to build a technology stack (the layers of hardware, software applications, operating platforms, and networks that make up IT architecture) to support current and future Internet of Things applications and devices, and whether companies should invest in open or proprietary technologies.

The transition from a traditional enterprise IT architecture to one optimized for the Internet of Things will not be easy. Elements of companies’ current technology stacks may need to be redesigned so they can support billions of interdependent processing events per year from millions of products, devices, and applications. Because networked devices are always on, companies must be able to react to customer and system requests in real time; agile software development and delivery will therefore become a critical competency. Seamless connectivity will also become a must-have, as will collaboration across IT and business units, which have traditionally been siloed. Moreover, companies must be able to securely and efficiently collect, analyze, and store the data emerging from these refined IT architectures.

Our work on digital transformation with companies in a range of industries suggests there are several critical areas companies will need to focus on to address these challenges—among them, actively participating in setting industry standards, exploring modular approaches to digital application design and maintenance, altering information collection and security protocols, and reconsidering how to manage existing products alongside newer Internet of Things applications and devices, as well as how to alter existing contracting processes to account for IoT service requirements.

Moreover, the complexity of Internet of Things technologies, the limited capabilities of many customers to implement them, and the need for interoperability and customization will provide numerous opportunities for hardware, software, and service providers to offer customers end-to-end IoT products and services (Exhibit 1). To do so, however, those companies may need to explore new operating models.

In this article, we consider the challenges and opportunities CEOs, CIOs, chief technology officers, and other corporate executives are facing as they seek to capitalize on the Internet of Things. We also look at the capabilities required to design, build, and support applications and devices that are part of an efficient and intelligent network.

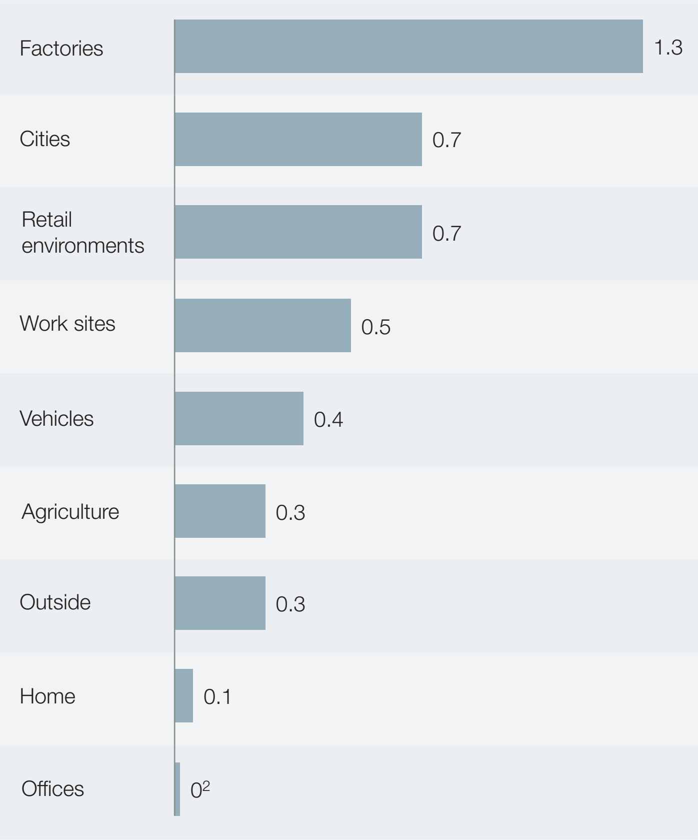
Retooling for the Internet of Things

Currently, there are more than nine billion connected devices around the world, including smartphones and computers, and that number is expected to at least triple over the next ten years.[3] However, most organizations are only just starting the process of upgrading their IT architectures and operating models to seize the potential business opportunities that all this connectivity presents—forward-thinking companies in the automotive and consumer-electronics industries notwithstanding. No question, making the switch is complicated and time consuming, but a focus on the following seven principles can help expedite the process.

Exhibit 1

Almost 40 percent of the $11.1 trillion economic impact of the Internet of Things requires interoperable systems—offering opportunities for hardware, software, and service providers.

Potential value that requires interoperability,[1] $ trillion



Examples of how interoperability enhances value

Factories	Data from different types of equipment can be used to improve line efficiency
Cities	Video, cell-phone data, and vehicle sensors can monitor traffic and optimize flow
Retail environments	Payment and item-detection systems can be linked for automatic checkout
Work sites	Worker and machinery location data can be linked to avoid accidents or exposure to chemicals
Vehicles	Equipment-usage data can be applied in insurance underwriting, maintenance, and presales analytics
Agriculture	Multiple sensor systems can improve farm management
Outside	Connected navigation can harness vehicles, GPS, and traffic control to enable greater driving precision
Home	Chore automation can be linked to security and energy systems to time usage
Offices	Data from different building systems and other buildings can improve security

[1] Includes sized applications only; includes consumer surplus; figures have been rounded.
[2] Less than $100 billion.

Source: McKinsey Global Institute analysis

Actively participate in setting technology standards

Current Internet of Things offerings are mostly based on proprietary data formats, service definitions, and interfaces, and they are tailored and optimized for specific uses. Many intelligent-lighting systems, for instance, use proprietary algorithms that allow a user to determine appropriate settings in a single home or office building, but these systems typically won't work with other home or office systems. New connectivity standards and common application programming interfaces will be required before an Internet of Things ecosystem truly can develop. Early movers have an opportunity to shape the game by partnering with universities, research bodies, and regulatory agencies to create new standards that will allow for expanded interoperability and modularity among and within devices and applications. AT&T, Cisco, GE, IBM, and Intel, for instance, cofounded the Industrial Internet Consortium. Its primary goal is to establish interoperability standards across industrial environments so that data about fleets, machines, and facilities can be accessed and shared more reliably. Other groups have been focused on standardizing the application programming interfaces that enable basic commands and data transfer among sensor-enabled devices.[4] By actively engaging in conversations about standards, companies can not only influence regulators but also be first to market with Internet of Things devices and applications and create new revenue streams from associated licensing efforts, thereby maintaining a firm grip on market share.

Factor connectivity issues into design

The question of where to embed "compute points" logically in products, applications, and devices will loom large for companies. Hundreds or even thousands of Internet of Things devices and applications may need to be connected to a wireless network at the same time. The average smart home, for instance, could contain 50 to 100 connected appliances, lights, thermostats, and other devices, each with its own power requirements. The average smart car may be gathering and processing hundreds of gigabytes of data per hour on traffic and travel—for instance, a camera at the front of the vehicle may be constantly capturing, assessing, and uploading to cloud servers information about stoplights and available parking meters. Depending on the overall amount of information being transmitted across broadband networks and the available bandwidth, these processing activities can be expensive for both customers and companies.

Companies' IT organizations and product engineers will need to develop clever solutions for "offloading" data when their devices are connected to broadband networks. They will need to carefully choose the optimal points along the data-processing journey at which data will be compressed, saved, or transmitted. Preprocessing of sensor data within Internet of Things devices may be one way to reduce bandwidth requirements. Automakers, for instance, might decide on a system design that stores traffic-related algorithms within individual cars' computing systems, so the vehicles will send only the most relevant data to cloud-based servers, thereby reducing the cost of transmission. The nature of broadband networks is that the cost to process data will change as bandwidth demand does; device design should be similarly flexible.

Embrace a continuous-delivery model for software and services

The replacement cycle for networked "things" may be longer than the innovation cycle for the sensors and software embedded within those products. Companies therefore should consider ways to upgrade their IT capabilities to enable continuous delivery of software updates. Modular designs will be required so IT engineers can refresh discrete components of an Internet of Things–connected device on a rolling basis without having to upgrade the whole thing. Tesla, for instance, developed a software- and sensor-based system that manages customer-service requests and administers fixes. When customers reported problems with rollbacks—stopping their cars on hills and then accelerating when the light changed—engineers at the company devised a workaround and delivered a firmware update to vehicles using broadband frequencies. The new Hill Start Assist feature was delivered online not just to customers reporting problems but also to all owners of Tesla's Model S vehicles.

To pursue a continuous-delivery model, companies will need to review their product-development processes and explore a "two speed" IT operating model. Under this approach, the IT organization would be simultaneously focused on supporting customer-facing applications that must be updated quickly and frequently—such as an auto-maintenance app—and "system of record" applications that are required to ensure stability and security. Such a model requires tight integration between IT operations and software-development groups within the company to ensure the speed and fidelity required from Internet of Things applications.[5] Additionally, new security schemes may be required for products that previously would not have been maintained, and therefore exposed, over the network. Finally, companies will need to develop the marketing capabilities required to communicate to customers the frequent need for upgrades—either through the IoT device or application itself or via alternative means, such as social media and online forums.

Consider retrofitting existing products and systems

As companies launch and update IoT products, they tend to build more and more complexity into their legacy IT architectures, and the newer devices are often incompatible with the existing product portfolio—relying on different data sets, for instance, and requiring separate maintenance schedules. However, older generations of a company's products and devices can still provide useful sensor data for the creation of new functions and features in younger generations of products. The computer systems in older-model jet engines or locomotives, for instance, may not be able to take advantage of IoT applications that allow for engine monitoring and "over the air" repairs. Nonetheless, these older systems contain a trove of mapping and other data that can be mined and used to further the development of IoT-based tracking services for transportation fleets. Companies will need to explore retrofit solutions so they can, at the very least, pull data from legacy products and systems. For instance, some automakers are using dongles and other devices to connect older-model vehicles to their assessment and maintenance systems when they come in for regular service. Companies may lack the skills required to use Internet of Things systems and data; they will need to find data scientists, R&D engineers, and managers who are trained in advanced analytics and have the ability to write custom algorithms.

Update cybersecurity strategy and privacy protocols

To reap the full value of Internet of Things applications and devices, and to be able to provide customized products and services to customers, it will be critical for companies to provide the highest possible levels of data security—after all, each device and interoperable product increases the "surface area" available for breaches, and every node is an entry point, so risks rise exponentially. A compromised IoT-based home security system or a disrupted medical monitor could pose life-and-death risks. A hacker's 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 (Exhibit 2).

Companies will need to establish trust with consumers, promote collaboration across companies and industries, and ensure the security of e-commerce platforms. In short, they will need to build what our colleagues have called "digital resilience," embedding methods of protecting critical information in their technology architectures, processes for business-model innovation, and interactions with customers.[6] There are specific technical interventions companies can take—for instance, investing in next-generation encryption of data and customer profiles and seeking ways to completely anonymize the data they collect. There are nontechnical enablers, as well—for example, publicly driven and monitored regulations and strictly enforced company security policies. Companies can embed customer opt-in and opt-out mechanisms in any Internet of Things device, product, or application throughout its life cycle. Perhaps most important, B2B and B2C customers need to see a strong value proposition for themselves in sharing potentially sensitive information from the start. Some insurers, for instance, have touted their ability to reduce premiums by up to 15 percent for a majority of customers through their analysis of individual drivers' usage data (rather than relying on actuarial tables).

Exhibit 2

Companies must ensure data are secure in the Internet of Things ecosystem.

	Category	Description	Example	How to address issues
Use of private information by companies, some of which has raised concerns	Control over data	Data given to companies cannot be deleted easily	Customer data are resold or are tied to operational data	Create transparency on collection and use of data, allowing customers to specify permitted uses
	Information imbalances	Companies have detailed customer information but are not transparent themselves	Retailers detect and use private information, eg, about pregnancy	
	Misleading data forecasts	Analyses have inherent faults that could lead to biases against individuals	Customer credit applications rejected due to duplicate names	
	Discrimination/ exclusion	Companies have knowledge to identify individual customer groups	Person loses health insurance when high cancer risk is detected	
Illegal activity by criminals	Data exploitation	Illegal exploitation of “back doors” or vulnerabilities	Private information is stolen	Ensure strong end-to-end security

Source: Österreichische Bundesarbeitskammer; McKinsey Global Institute analysis

Explore modularity, interoperability, and open-source technologies

To expand their universe of partners, companies should consider building modular Internet of Things stacks (mirroring the modular product and device designs we discussed earlier) with open-source components that can stand alone. Some companies, for instance, are already building open source–based platforms for data processing that can be maintained and further developed by different systems integrators. Many companies are also actively contributing to open-source software development by making all or parts of their proprietary development efforts publicly available. Almost all the components in a typical IoT technology stack can be maintained using open-source software, but in some instances companies will still want to consider questions of cost, performance, and stability before deciding whether to use proprietary software or open source.

Companies won’t be able to easily bolt new Internet of Things technology stacks onto their existing IT architecture; older systems may not be able to handle the massive traffic and usage associated with networked products. There are several different integration models they can explore. In some cases, a one-time copy of critical data from the older system may be sufficient to kick-start an Internet of Things stack. In other cases, companies may need to build data-integration layers into existing stacks to facilitate the flow of common data to multiple stacks within the architecture. The IoT technology stack may either operate completely autonomously or be integrated more tightly with the rest of the IT architecture, depending on the level of data exchange desired. Flexibility is critical; the IoT stack must be able to be deployed in slightly different infrastructure setups, in multiple regions, and should account for country-specific settings related to data privacy and data storage.

Consider different organizational structures

Most Silicon Valley firms have embraced agile software-development methodologies and organizational structures. By contrast, many traditional, hardware-driven companies still hew closely to a “statement of work” model; rather than build software in-house, these companies share specifications with systems integrators that do the development. In an IoT world where products, devices, and applications must be updated quickly and frequently, this organizational model has limitations. Companies may want to explore different organizational structures to enable agile software development, whether that process happens in-house or through closer collaboration with systems integrators. Establishing a start-up environment within the company can be effective for encouraging such internal innovation and promoting joint efforts from the product-development and IT operations groups (commonly referred to as a DevOps approach to product development).[7] Traditionally, the IT organization has been distinct from operations; in the retail context, for instance, the IT function manages back-end point-of-sale systems, while the operations group manages the physical store. But IT is now embedded in everything businesses do and directly affects the metrics by which operations are measured, so it only makes sense for those functions to be more closely aligned.

Indeed, companies will need to break down organizational silos: product developers cannot learn from customer-usage data that remain locked up in the service department. Information must be shared freely among departments and functions, and ownership rights to the data produced by various connected devices must be established and communicated.

The Internet of Things is only now gaining full steam. Companies that can retool their IT architectures to capitalize on this connectivity trend have a tremendous opportunity to create new sources of value for customers and enjoy sustainable financial and operational benefits. ■

[1] "Economic impact" is defined in the report as the collective financial and nonfinancial benefits end users may gain from the use of Internet of Things applications.

[2] For more, see "Unlocking the potential of the Internet of Things," McKinsey Global Institute, June 2015, on mckinsey.com; and Jacques Bughin, Michael Chui, and James Manyika, "An executive's guide to the Internet of Things," *McKinsey Quarterly*, August 2015, mckinsey.com.

[3] For more, see "Unlocking the potential of the Internet of Things," McKinsey Global Institute, June 2015, on mckinsey.com.

[4] Harald Bauer, Mark Patel, and Jan Veira, "The Internet of Things: Sizing up the opportunity," *McKinsey on Semiconductors*, December 2014, mckinsey.com.

[5] Oliver Bossert, Chris Ip, and Jürgen Laartz, "A two-speed IT architecture for the digital enterprise," *McKinsey on Business Technology*, December 2014, mckinsey.com.

[6] Tucker Bailey, James M. Kaplan, Alan Marcus, Derek O'Halloran, and Chris Rezek, *Beyond Cybersecurity: Protecting Your Digital Business*, first edition, Hoboken, NJ: John Wiley & Sons, April 2015.

[7] Satty Bhens, Ling Lau, and Shahar Markovitch, "Finding the speed to innovate," *McKinsey on Business Technology*, April 2015, mckinsey.com.

Johannes Deichmann is a consultant in McKinsey's Stuttgart office, **Matthias Roggendorf** is a senior expert in the Berlin office, and **Dominik Wee** is a principal in the Munich office.