Achieving Strategic Objectives Through Successful IoT Implementation

By Raj Krishnamoorthy, FCA, CPA

Raj is a Partner in the Cyber Risk (Risk Advisory) practice with Deloitte. With over 30 years of experience. Raj leads the Managed Security Services area within Cyber in Canada. The Managed Security Services practice helps organizations manage the security risks associated with their Security infrastructure. He holds a CISSP and CISA. Raj has led many projects involving Managed Security Services and helping clients solve complex Cyber issues.

An air-conditioning unit in your building begins to underperform. You are able to analyze its performance trend through a specific duration and realize that there is a leak in the gas pipe that's causing the unit to work below capacity. Your process automatically raises a ticket to your operation team's helpdesk and you remotely prioritize and route your maintenance staff to attend to this issue. Simultaneously, you are able to alert your A/C supplier of the irregularity, either through email or other channels, enabling the business to keep track of product performance over time and schedule replacements if required.

> Managing a range of complex protocols, interfaces, hardware and standards from around the world can be daunting for an organization dealing with connected platform products.

You see how data consolidation takes place and, by building a unified, common ground (of sensors, gateways and platform-enabled software), and you begin to converge and derive profitable value from both these worlds, enabling data to interact and interoperate across legacy and newer systems. Replace the A/C with critical operational components and machinery, and the example will hold for a seamless and automated process for either preventing and/or detecting failures or reacting to it efficiently. All this is possible by the group of technologies often referred to as Internet of Things (IoT)

"The Internet of Things connects people, places, and products and, in so doing, it offers opportunities of value creation and capture for a full panoply of stakeholders. Organizations, however, should be careful to focus on IoT initiatives that solve real business problems and create real business value – not just connecting stuff for the sake of connecting stuff."[1]

Today, it seems easy to imagine a world in which a manufacturing enterprise enjoys complete visibility and monitoring of inventory as it enters the factory, gets processed, and leaves the factory floor. Or (imagine) a world where it is possible to remotely track and optimize production asset effectiveness – through introduction, maintenance, and retirement – and even detect system failures as they occur to maximize uptime. Or still, another world in which products are given sensor capabilities to detect usage patterns and, on that basis, inspire still more products and revenue streams.

It is easy to imagine these and other such worlds because it is in fact the world of smart connectivity within which we live today, thanks to the capabilities offered by the IoT.
But it wasn't always so easy or so "obvious."

A Bit of History

In 1991, long before anyone ever used the term "Internet of Things," Mark Weiser, chief scientist at Xerox, imagined a world of "ubiquitous computing" in which all objects could sense, communicate, analyze and act with respect to other objects and people.[2] But it was only in 1999 that the term "Internet of Things" was coined by Kevin Ashton, a technologist specializing in sensors and radio-frequency identification (RFID) tags.[3] Over the years since then, we have witnessed various IoT applications evolve from concept to fruition across the full range of industries and use cases.[4]

This primer provides an overview of the IoT: its market space, key drivers, underlying challenges, potential solutions and the business value it creates. The piece is intended to help readers understand at a high level why they should proceed in considering the technology's current and potential business applications and associated benefits and outcomes.

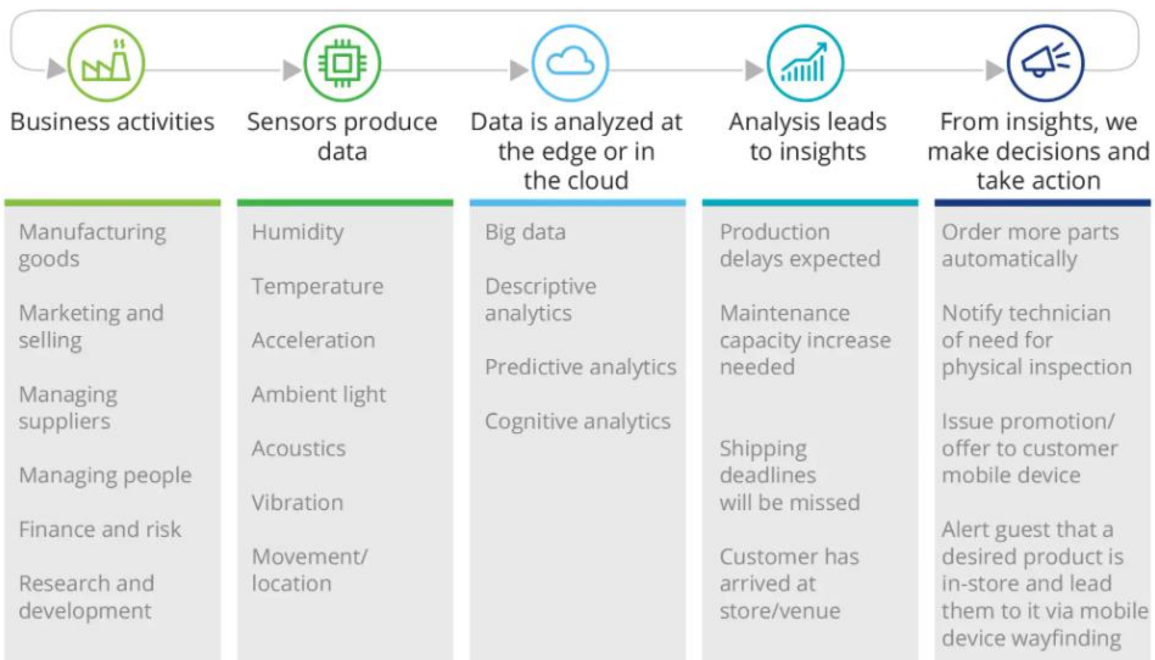
There are several definitions of the IoT in technical literature and popular media:

The IoT is a suite of technologies and applications that equip devices and locations to generate all kinds of information – and to connect those devices and locations for instant data analysis and, ideally, "smart" action. Conceptually, the IoT implies physical objects being able to utilize the Internet backbone to communicate data about their condition, position, or other attributes.[5]

Creating and Capturing Value

The IoT focuses on the aggregation and use of information from several sources. Information, however, creates value only when it is utilized for modifying future action in beneficial ways. Ideally, this modified action gives rise to new information, allowing the learning process to continue. Information can then create value not in a linear value chain of process steps but, rather, in a never-ending process. One way of capturing this process is as an Information Value Cycle (IVC) with discrete but connected stages (figure 1).

Figure 1. IoT Information Value Cycle



Source: Deloitte Consulting LLP.

Deloitte Insights | deloitte.com/insights

For information to complete the cycle and create value, it passes through the cycle's stages, each enabled by specific technologies.[6] It starts with everyday business activities that generate data. This data is captured by sensors (attached to devices), creating information as a result, along an array of dimensions from vibration to humidity to movement, and beyond. Such information is communicated via a network, aggregated, and analyzed, leading to insights. These insights—sometimes called "augmented intelligence"—may then either enable automated action or shape human decisions ("augmented behavior") in a manner leading to improved, more competitive business operations, thereby completing the cycle.[7]

Characterizing the IoT Market Structure

When one thinks at a very high level, IoT market segments can be generally divided into three broad categories: enterprise/industrial, consumer and services/public sector. Each of these segments is marked by distinct characteristics and market opportunities (Table 1).

Table 1. IoT market structure

	Enterprise/industrial	Consumer	Services/public sector
Representative value opportunities	• Planning and inventory • Factory and operations • Supply network and logistics • New business models • New products and product development • Asset management	• Customer experience • Channel connectivity • Aftermarket support • New products and extensions • Lifestyle enhancement	• Health care delivery • Commercial building energy management • Public sector safety • Public sector traffic management • Crop yield management
Representative use cases	• Demand and supply synchronization • Quality sensing and prediction • Condition-based monitoring • Dynamic routing and scheduling	• Smart homes • Remote appliances • Connected cars • Personal lifestyle monitoring • Personal asset tracking	• Smart buildings • Smart cities • Smart irrigation • Patient surveillance • Smart law enforcement
Additional features	• Manufacturing operations and product driven • Private cloud primarily • Hybrid architecture • Fewer devices • Relatively complex data sets • B2B channels	• Customer and product driven • Public cloud primarily • Millions of devices • Simpler data sets • B2C channels	• Public sector, services driven • Public/private cloud mix • Variable data set complexity • Medium number of devices • B2B2B, B2B, B2C channels
Projected global IoT spending share by 2020	50–60%	20–25%	20–25%

Source: Deloitte analysis. **Deloitte Insights | deloitte.com/insights**

The enterprise/industrial segment involves relatively complex and rich data sets and far fewer devices relative to the consumer segment. The enterprise/industrial segment tends to also be driven by manufacturing operations and product development within a relatively private cloud environment. In contrast, the consumer segment is typically rooted in customer experience and a more public cloud environment. The services/public sector segment is generally something of a hybrid between the other two segments in terms of richness and complexity of data, number of devices and a bias toward a particular cloud environment, although it tends to bear a closer resemblance to the consumer segment in terms of experience-driven use cases.

The fastest growing IoT segment appears to be enterprise/industrial, projected to capture slightly more than half of global IoT spending by the end of 2020. A particularly strong driver of growth in IoT spending within the enterprise/industrial segment is digital supply network (DSN) applications. While there is a host of DSN use cases that is driving IoT spending within the enterprise/industrial segment, four seem to stand out in particular:

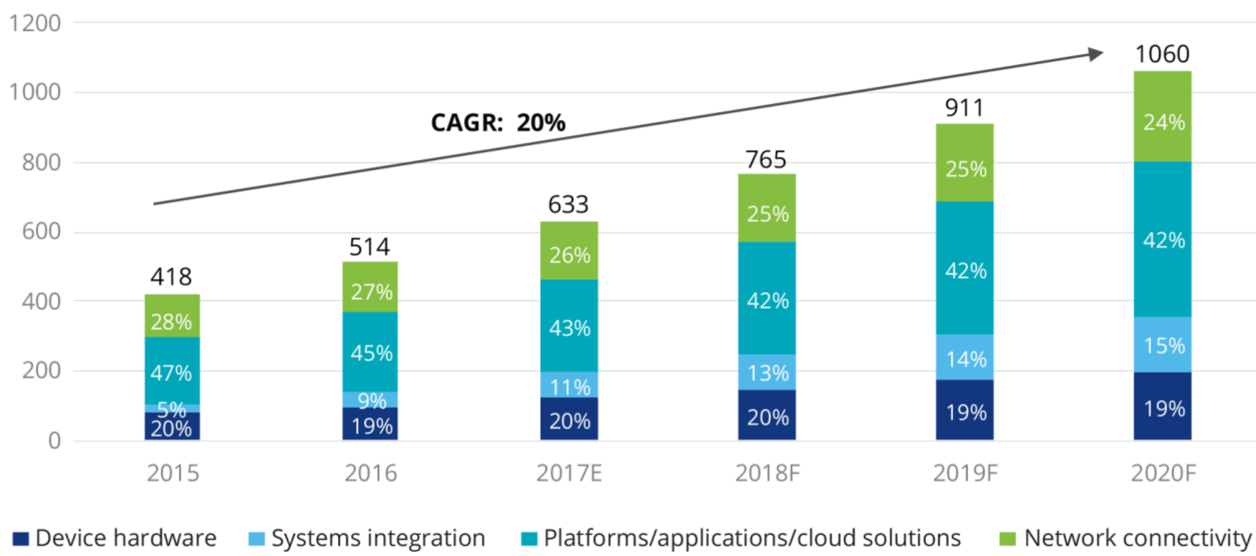
- *Condition-based monitoring/predictive maintenance*: Monitoring and continuously evaluating key performance parameters of capital assets and, in the process, leveraging advanced analytics to predict failures before they occur.
- *Asset tracking:* Tracking location and movement of assets and/or materials using location-based sensors, enabling real-time reporting and optimization of system performance.
- *Dynamic routing and scheduling*: Enhancing the productivity of both individual units and broad networks using deep and broad insights derived from aspects such as visibility on conditions and performance in real time
- *Asset and process optimization*: Evaluating and monitoring operational data and ambient conditions of critical assets and processes in real time to optimize performance and safety manufacturing is a substantial driver of spending within the enterprise/industrial IoT space and overall IoT spending.[8] This may be attributed to Industry 4.0 and the ensuing wave of digital transformations that will likely drive significant demand for IoT capabilities across a broad spectrum of services within manufacturing. Other key sectors driving enterprise/industrial IoT include oil & gas, power & utilities, life sciences/health care and transportation.

Quantifying the IoT Market Potential

The IoT is a complex ecosystem and there are different approaches to its market sizing. One of the common ways of describing the market is in terms of connected devices. In 2016, the number of IoT-connected devices was estimated at 18 billion units and is expected to grow at approximately 15% CAGR to reach about 31 billion units by the end of 2020.[9] Other estimates place the projected number of connected devices at somewhat less than this figure.

Alternatively and without regard to the end-use segment, the IoT market can be characterized in terms of four categories of products – device hardware, systems integration, network connectivity and platforms/applications/cloud solutions.[10] These four categories taken together (which comprise the global IoT market) had an estimated market value of $0.4 trillion in 2015, and is forecasted to expand at approximately at a 20% compound annual growth rate (CAGR) to reach around $1.1 trillion in 2020 (Figure 2).[11] As mentioned, the enterprise/industrial sector is expected to account for by far the largest share of this global IoT market in 2020 at about 50 to 60% of total spending.[12]

Figure 2. Forecasted global IoT market spending ($ billion)



Source: Jenny Lai, Anderson Chow, Carrie Liu, and Chi Tsang, *The industrial Internet of Things*, HSBC Global Research, November 2016, p. 14.

Deloitte Insights | deloitte.com/insights

While some key factors seem to be driving the growth of the IoT, we should be mindful of some of the issues hindering IoT applications, and their corresponding potential solutions. Table 2 offers a set of some of the technical challenges that confront continued IoT development.

Table 2. Representative technical challenges for growth of IoT and potential solutions

Technical area	Challenges	Potential solutions
Sensors	Interoperability issues in heterogeneous sensor systems	Constrained Application Protocol (CoAP) and Hypertext Transfer Protocol (HTTP) may facilitate communication between heterogeneous sensor systems.[17]
	Security issues	Complex cryptographic algorithms may ensure data integrity within sensors.
	Impractical or expensive power consumption	Advancements in silicon technologies and alternative energy harvesting may improve cost efficiencies.[18]
Network	Security	The Internet Protocol Security (IPSec) suite provides a certain level of secured IP connection between devices.
	Power consumption	Power-aware routing and sleep-scheduling protocols may improve power management in data-intensive networks.[19]
Standards	Underdeveloped legal, regulatory, and technical standards on a global scale	Although companies are collaborating with consortia (e.g., Industrial Internet Consortium [IIC], oneM2M) to develop legal and regulatory standards, much work remains. Stakeholders within the global IoT ecosystem should make the creation and implementation of standards an utmost priority.
Data analytics	Technical skills to leverage newer big data tools[20]	Engineers are being trained to use newer tools such as Spark and MapReduce in order to tackle the need to use unstructured data.[21]
Augmented intelligence	Legacy systems' ability to process real-time and unstructured data	Predictive applications could be designed to use a combination of batch processing (data is aggregated in batches and then processed) and real-time processing to draw meaningful conclusions.[22] Newer analytical tools discussed earlier in the paper highlight opportunities to make use of unstructured data for meaningful decision-making.
Augmented behavior	Lack of interoperability in a machine-to-machine (M2M) setup	There is a need for convergence of standards with support from different stakeholders within the IoT ecosystem so that machines with heterogeneous brands, hardware, software, and network connections can interoperate.
	Machine judgments in unstructured situations and human use of insights	Continuously improving statistical tools and algorithms bring the machine's decision-making ability closer to reality, making it simple for business users to comprehend the results through easy-to-use visualization tools.

Source: Jonathan Holdowsky, Monika Mahto, Michael E. Raynor, and Mark Cotteleer, *Inside the Internet of Things (IoT)*, Deloitte University Press, August 21, 2015.

Deloitte Insights | deloitte.com/insights

Managing a range of complex protocols, interfaces, hardware and standards from around the world can be daunting for an organization dealing with connected platform products (IoT).

Organizations often feel like they are drowning in a sea of different domains such as hardware, firmware, web, mobile and cloud, which ultimately becomes a roadblock for their usual business. Typical challenges in IoT security testing faced by organizations are highlighted below.

Component	Typical challenges
Increase in Adoption	Increased adoption of IOT enabled devices across various industries and sectors.
	Increase in adoption of Cloud-based solutions in various industries and sectors.
Increase in Security and Privacy Concerns	Increasing concerns relating to security of devices and data privacy in the connected world.
	Increase in cyber-attacks and targeted attacks on IoT devices and solutions.
Inadequate Security Measures	Lack of inherent security and privacy measures embedded into IoT devices and services.
	Lack of knowledge of reliable industry standards and regulations relating to IoT device security compliance.
Insufficient Expertise	Lack of knowledge of protocols and interfaces used in IoT devices and products.
	Lack of professionals with sufficient experience or knowledge of IoT and security embedded design principles.

Key Considerations for Organizations

The IoT is emerging as an important digital transformation technology irrespective of industry, business function or geography. Costs associated with data collection, transfer, processing, storage and computing have together come down to a point where they can drive significant mainstream IoT applications. With fast-evolving and expanding applications, the IoT seems to be shaping into an increasingly complex ecosystem that offers opportunities of value creation and capture for different stakeholders, including individuals, societies, companies, consortia and governments. As such, the IoT is increasingly influencing the way we run businesses and live our lives. Additionally, the IoT is also expected to drive and support a number of related yet different technologies such as augmented/virtual reality, automation and robotics.

All of this said, however, organizations should bear in mind that “connectivity” *in and of itself* is not a strategy that necessarily provides real business value. Unfortunately, many IoT initiatives end up being “shiny” solutions in search of a problem, concepts that have popular appeal but don’t deliver real-world value. And organizations *should* be focusing on IoT initiatives that create real business value, not just connecting stuff for the sake of connecting stuff.
Indeed, the real power of the IoT likely resides in harnessing its incredible potential in solving *real* problems and, in so doing, creating *real* business value. From asset monitoring and predictive maintenance to fleet management and logistics to smart supply chains to smart mobility and well beyond, the IoT – when used strategically – can help solve some of the most nettlesome challenges that organizations of all kinds face today. As IoT applications are evolving

with each passing day, companies may wish to think through their current and future strategic positioning and build product and service offerings accordingly.

And toward that end, companies can adopt a commonsense approach in implementing IoT solutions successfully. First, companies should *think big*. Push the envelope in developing an ambitious and forward-looking IoT vision that cuts across organizational silos. Second, companies should actually *start small*. Target the most promising opportunity areas, launch small and swiftly and go for the rapid wins. Third, companies should *scale fast*. Once an IoT initiative is proven successful, companies should scale up quickly to maximize benefits. Finally, companies should consider turnkey solutions that may help to jump-start the process – solutions that are geared toward a particular industry or business application in line with the organization's objectives.

There is no magic formula when it comes to successful IoT implementation. But companies that know what they want to achieve in relying on the IoT – and approach it with a vision that is grounded in real-world issues – may very well have a leg up in achieving strategic objectives.

1 "The Internet of Things: A Technical Primer," *Deloitte Insights* (February 2018).
[2] Michael E. Raynor and Mark Cotteleer, *The more things change: Value creation, value capture, and the Internet of Things*, Deloitte University Press (July 27, 2015). View in article.
[3] Jim Eckenrode, *The derivative effect: How financial services can make IoT technology pay off The Internet of Things in the financial services industry*, Deloitte University Press (October 13, 2015). View in article.
[4] Deloitte analysis; Airbus, "Airbus moves forward with its "factory of the future" concept," accessed October 12, 2017; IoT Agenda, " How IoT will change auto insurance," accessed October 17, 2017; Andrew Meola, "Automotive industry trends: IoT connected smart cars & vehicles," *Business Insider* (December 20, 2016); other analyst reports. View in article
[5] Surabhi Kejriwal and Saurabh Mahajan, *Smart buildings: How IoT technology aims to add value for real estate companies*, Deloitte University Press (April 19, 2016). View in article.
[6] The elements of each stage of the IVC in Figure 1 are presented for illustrative purposes. View in article.
[7] *Ibid*.
[8] Jenny Lai, Anderson Chow, Carrie Liu and Chi Tsang, *The industrial Internet of Things*, *HSBC Global Research* (November 2016), p. 14. View in article.
[9] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," accessed November 1, 2017. View in article.
[10] Lai, Chow, Liu, and Tsang, *The industrial Internet of Things*, p. 14. View in article.
[11] *Ibid*, p. 8 and p. 13.
[12] *Ibid*, p. 14.