1

Beyond the Hype—All You Actually Need to Know About IoT for Business

Like it or not, the Internet of Things (IoT) will change your organization unlike anything before. It will change your organization more than business process reengineering (BPR), Six Sigma, lean manufacturing, agile computing, or any of the other business concepts that periodically pop up, experience success, and are forgotten when the next big thing arrives. Granted, to date most of IoT deployments have been incremental and evolutionary, streamlining an existing process here, cutting some costs or improving productivity there. That, however, is about to change as IoT ramps up, as standards are adopted, and as security is bolstered—all of which and more are in the works. So please don't misunderstand me. The Internet of Things certainly will be a big thing—an enormously big thing, actually. But it isn't *just* the next big thing. IoT is the future—your industry's future, your organization's future, and probably your personal future. Welcome to the future. It's spelled I-o-T. All this may seem like hype now, but it will prove in the end to be quite understated; IoT is very, very real.

You still are skeptical. The hype around IoT certainly has become deafening and distracting. Over the past few years, however, I have traveled more than a million miles meeting with people around the world to discuss IoT. Some of those people have actually done stunning things with IoT and wanted to show these off for me. Others were struggling with a problem IoT should be able to solve and wanted to know how their peers were doing it. Full disclosure: not every business problem, it turns out, lends itself to an IoT solution.

OK, so are there problems I wouldn't recommend an IoT solution for? Not many come to mind immediately. If you insist, for starters there is the connected home. At the Consumer Electronics Show in Las Vegas you can see home appliances from washing machines to coffee makers connected to the Internet and to each other. The problem: while I see value in connecting individual home devices to the Internet, the business case for connecting all appliances and devices to each other in the mainstream home is just not there yet. There are a few emerging use cases, for example, home security and elder care where specialized devices in the home have to be interconnected, but an immediate IoT payoff is still some distance away.

In truth, most of the current implementations of IoT are in the business-to-business (B2B) area and are focused on improved efficiency and productivity around existing processes. As I said, IoT gains are incremental at this point. The real payoff from IoT comes down to automating existing processes that have a large labor or time component and streamlining the related process in one way or another. The resulting improvements, despite having measureable business impact, are mostly evolutionary. Similarly, you, too, after reading this book, should focus first on streamlining and improving your existing processes, which will deliver your fast paybacks and set you on the path toward more revolutionary applications, new business models, and incremental revenue streams. For example, you might use IoT to automate a data collection process you now do manually or remotely monitor something that otherwise requires a person to actually visit. Such solutions are already well proven and documented. I do, however, expect that down the road many breakthroughs in IoT will also come from the B2B2C (business to business to consumer) domain, but today they are just starting to emerge, pioneered by early adopters: processes like mass customization, food safety, and even autonomic car or drone transportation/delivery (see Figure 1.1).

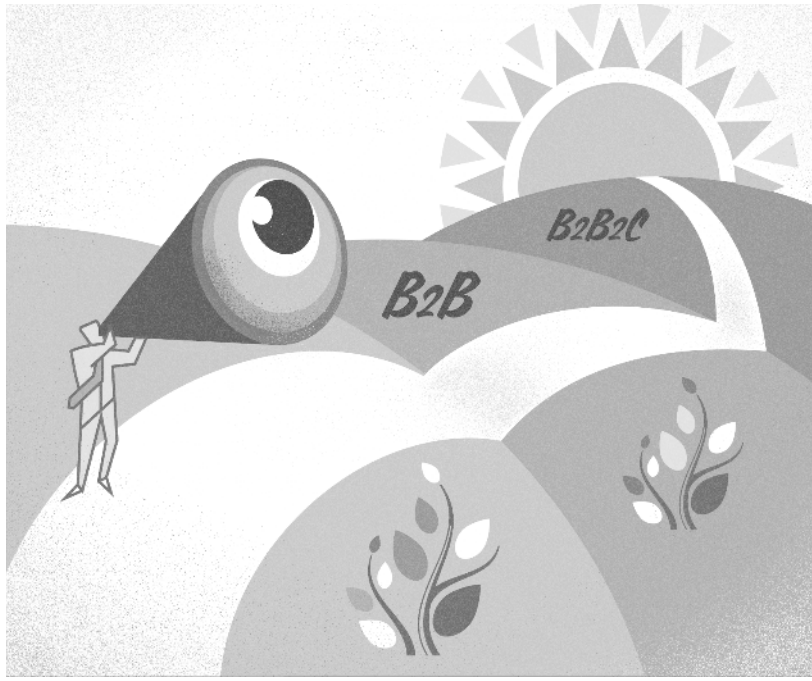

Figure 1.1 B2B and B2B2C Domains

In the meantime, manufacturing around the world, including in North America, is having a renaissance of sorts, and IoT is part of the reason. By converging previously siloed sensors, machines, cells, and zones, IoT-driven factory automation helps enterprises integrate production and business systems and then bring everything online over a single network. Organizations are gaining flexibility to quickly adapt to changes, whether for new product introductions, planned product line changeovers, or other adjustments. Each affected zone, from the enterprise to the plant floor to the loading dock, receives real-time alerts about changes through networked mobile devices, video monitors, and human-machine interfaces. The real-time information also links back to the entire supply chain, so each step in the manufacturing value chain, from supply through production to distribution, can respond as quickly as needed.

These represent evolutionary improvements that together deliver real business value. Similar gains are being achieved in transportation,

utilities, agriculture, building automation, education, retail, health care, sports, and entertainment—even the military. Companies in these industries are taking first steps on their IoT journeys starting with low-hanging fruit. Still, the process improvements are real and the paybacks, the ROI, add up to serious money in the bank, as I will demonstrate in Chapters 3 and 4.

So this isn't theory. It's real, and it's working today. What a better example than a legendary American motorcycle manufacturer, Harley-Davidson Motor Company. The company was facing intense global competition while its core market was aging and new younger buyers wanted a different type of motorcycle.[1] It needed to get agile, to be able to respond to changes fast, and to be more efficient and productive. IoT gave Harley-Davidson the capabilities it needed. Here's how.

Harley-Davidson faced the familiar litany of problems encountered by many American businesses, especially large and market-leading companies or those with ambitions to be so in their industry. Labor was too costly. Production was not aligned with IT operations. Islands of incompatible data were everywhere. "You name it, we suffered from it," one former Harley manager told me.

So the company pulled together key people from both IT and operations (known as operational technology, or OT). In every industry and most businesses, IT and OT are notoriously uncooperative, almost as if IT, as the book title says, was from Venus and OT from Mars. We're not talking about a mass revolution here: more like a couple of people from different groups who got together by themselves and started actually talking to each other. Later they pulled in a few others and sat together in a room until they formed a unified team willing to communicate with each other and with other Harley-Davidson business units to gain the efficiencies IoT could deliver. The company converged its multiple networks into a single network and began consolidating data islands. As of this writing, one Harley-Davidson factory is fully IoT-enabled. The results are impressive. "What used to take a painfully long time to triage and troubleshoot now can be accomplished in a single morning," the manager said, an order of magnitude improvement. That alone led to increased productivity, efficiency, flexibility, and agility. The results have been so astonishing that other Harley-Davidson factories are clamoring to be the next adopters of IoT.

Moreover, those are just the operational results. Harley-Davidson's strategic business outcomes from the IoT-induced changes are equally impressive:

- Eighty percent faster decision making due to workforce enablement
- Dramatic reductions in costs and set-up time
- Continuous asset management, enabling even better decision making
- 6.8 percent increase in production throughput due to asset tagging
- Ten to 25 times improvement in build-to-order (BTO) cycle times (18 months reduced to two weeks)
- Seven to 12 percent increase in IoT automation-driven equipment utilization

All of this led to a profitability increase between 3 and 4 percent. And that was just one factory!

Harley-Davidson bet its future survival on IoT and, from its first IoT-enabled factory, it began paying off big (see Figure 1.2). This same future attracts what I refer to as Generation IoT everywhere.

Generation IoT Drives Business Survival in the 21st Century

If you look at the last 25 years of the tech industry, you'll see that change has been constant. Every three to seven years, organizations had to reinvent themselves. Companies that missed one technology transition could possibly recover if they scrambled to catch up. Those that missed two, however, most likely perished. Interestingly, according to The Boston Consulting Group, when you look at the roster of S&P 500 companies from 50 years ago, only 19 percent are still in existence.[2] The rest have perished.

As the S&P 500's mortality shows, we're so used to change that we barely notice it occurring. Remember tape recorders, CDs, VHS tapes, and answering machines? The advent of each changed society in substantive ways. When I asked my children about CDs and VHS tapes, I got blank stares. What about home telephones? I recently met a teenager who didn't recognize a telephone busy signal when she heard it; she had never experienced the phenomenon. When it was explained, she was baffled.

Figure 1.2 Harley-Davidson Case

Everyone has voicemail and call waiting, she insisted. Tape recorders, CDs, VHS tapes, and answering machines are maybe 30 years old, and yet they're not only obsolete but also now forgotten. Their replacements are now integrated into your smartphone. Society and business keep moving forward.

This is as good a point as any to tell you about me, your author. Obviously I'm a father with a bunch of kids, but what's important to you is my experience with IoT. My IoT journey started 12 years ago as a manager at Cisco when several of us flew to Cleveland and started working on industrial Ethernet switches together with Rockwell Automation. It was a challenging assignment for our team, encompassing a completely new set of requirements, certifications, and accommodating so many ruggedized systems versions, but we got things to work. A few years later, we decided that the time was right for Cisco to focus on the industrial networking segment, and we created the Connected Industries Group, which I ran. We also decided to adopt the IoT term to describe the phenomenon of everything connecting to everything. Anyway, this is how I started.

From there our plan for IoT was to expand our ruggedized infrastructure portfolio, develop vertical solutions expertise, build a partner ecosystem to augment our own skills—even then we realized that IoT would be bigger than any one organization could do on its own—and offer a platform for real-time analytics and vertical applications. We also evangelized IoT to the rest of the industry with the goal of getting them excited about its potential so that together we could turn the IoT vision into a huge market opportunity for everybody. Judging from the latest independent industry projections of billions of connected devices in just a few years and trillions in revenue, it has worked out pretty well to date. The important part, however, is that we have started to deliver on that promise. Now, if you haven't done so already, I hope that after reading this book you will join us as well by introducing your organization to IoT and participate in the IoT economy.

Today, the pace of change is more than a constant; it's the new status quo. The Millennials now entering the workforce know only unrelenting change. To them it's a way of life, one that will likely continue for the rest of their lives. But no matter our actual age, we are all part of a generation poised to encounter revolutionary change. That's why I call what we're experiencing in every business segment Generation IoT.

So how does your business survive in this environment? How do you avoid the mortality we've seen among the S&P 500? That's what this book is about—understanding this emerging change that has just begun to sweep over us and finding a strategy that will ensure your business and your career not only survive but thrive. The winners in this new era will recognize the changes occurring around us and be willing to adjust and re-learn, over and over again. They are Generation IoT.

So how do we spot these winners? You belong to Generation IoT if you embrace open standards, open collaboration, open communications, and open, flexible business models and you're willing to assemble a comprehensive partner ecosystem to build and deploy agile, flexible business solutions. The losers, however, will insistently stick to the old ways of doing business or try to do it all themselves. We've seen them many times in the past. They run their operations on proprietary or semi-standard technologies and adopt business models that lock in customers, ultimately destroying whatever value they initially delivered.

Need another example of IoT-led transformation? How about Ford Motor Company, a major U.S. automaker? It hasn't been long since the company together with its peers was on the ropes during the financial crises. Today, Ford has smartened up and changed processes. Of its 40 vehicle assembly plants, 25 now use IoT technology to speed communications within and between them. Plants around the world are now connected to the Ford enterprise network. Moreover, its next-generation automated vehicle scheduling system manages production in real time, handling more than 2 million variations. As a result, Ford is selling more cars than ever before. Thank you, IoT.

First Step on IoT Security Journey

The ability to deal effectively with security threats is the number 1 make-or-break factor for IoT adoption. Without it, companies will be reluctant to implement IoT and thus not benefit from the growing number of powerful use cases emerging across all industries.

The industry recognizes the challenge and is making it the top priority. IoT security is starting to be integrated into the very fabric

of both industry and public infrastructure, including fundamental areas such as transportation and logistics, power grids, water supplies, and public safety. However, much more needs to be done. We still lack skills, education, and awareness. Many companies continue to be in denial, still relying on a discredited physical separation approach to securing their plants and infrastructure. The OT and IT divide prevents the companies from implementing modern and proven security best practices.

So how should organizations start to approach IoT security? According to Verizon's "2015 Data Breach Investigations Report," most security breaches exploit well-known vulnerabilities where companies have not applied available fixes. The first step, therefore, is to implement existing best practices by following these three sets of guidelines:

- **Adopt** a single policy-based security architecture built on an open, unified approach with automated, risk-based self-defense and self-healing capabilities.
- **Converge** around standards. Vendors and enterprises alike need to leverage IT industry standards and best practices in OT and to fill in the gaps between industry-specific and horizontal standards organizations.
- **Collaborate.** OT, IT, information security teams (CiSO), together with vendors and consultants, must work together on common architectures, incorporating not only OT requirements into the IT provider's product portfolio but also supporting form-factors, up-time requirements, and integration with legacy industrial protocols. Security isn't your differentiation; it's your foundation. Therefore, let's learn and share together.

Yes, IoT is different than IT in many ways: it is more distributed, more heterogeneous, and more dynamic. There are many new IoT scenarios that require brand new approaches to security. We will explore them in more detail in Chapter 9. But the first step on the IoT security journey is to leverage 30+ years of experience and best practices that IT security systems give us. So let's not reinvent the wheel.

A Revolutionary Economic Opportunity

Many of us view IoT as the next stage of the Internet/Web that uses the Internet protocol–based (IP-based) distributed cloud to connect anything to anything. According to Vernon Turner, senior vice president of enterprise systems and IDC Fellow for The Internet of Things, "Think of IoT as a network of uniquely identifiable things that communicate using IP connectivity without human interaction." Pretty straightforward, huh? Some people, including me, extend this definition into what some call the *Internet of Everything (IoE)*, a term first coined by Cisco, or even to the digitization of smart assets. IoE brings together the people, processes, data, and things that make networked connections more relevant by turning information into actions. For the purposes of simplicity and clarity, this book refers to both IoE and IoT as IoT—in effect, treating the two terms as synonymous.

Here's an easy way to think of what's going on: The first stage of the Internet connected people to networks, data, each other, and processes. With IoT, we're now connecting anything with anything—or, if you prefer, everything with everything. In short, anything that can be digitized can be part of IoT. The business impact of IoT makes it revolutionary; when everything can communicate with everything else, it essentially redefines and creates new business value chains (see Figure 1.3).

First, as Turner points out, IoT disrupts traditional value chains. This forces companies to rethink and retool everything they do, including product design, production, marketing, and after-sales service, while using analytics combined with security. That's essentially what happened at Harley-Davidson. From there, smart connected products expand traditional B2B channels and effectively demolish line-of-business (LOB) boundaries.

A decade ago, visionaries talked about mass customization—the ability to customize mass-produced products to each individual buyer's specifications. A few tried, but it proved very difficult to implement efficiently. The process had too much latency (delay), which added cost and slowed the results. However, IoT makes strategies like mass customization far more practical and cost efficient. Latency isn't a problem. Information can be shared in real time between every element in the supply chain. Buyers can click on the components they want. Suppliers and logistics providers

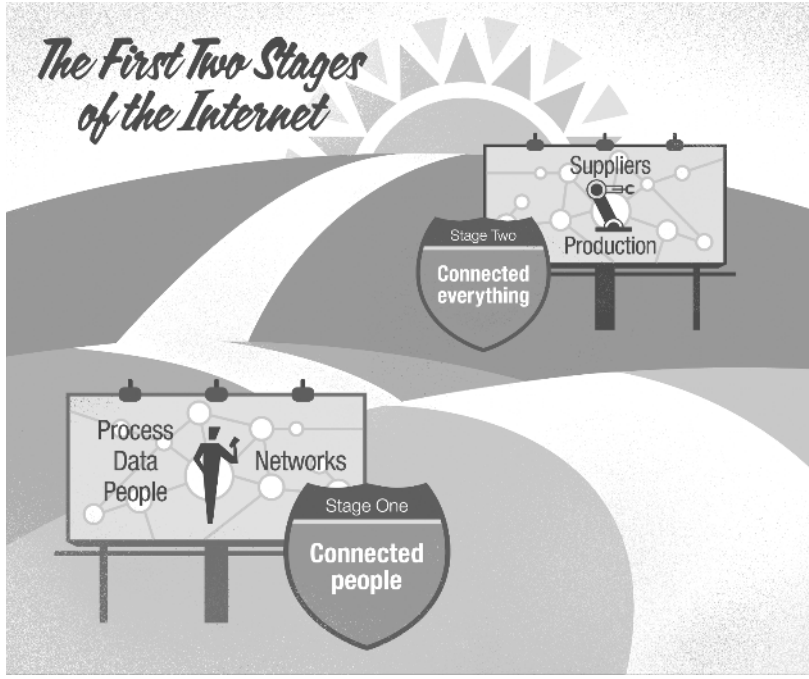

Figure 1.3 First Two Stages of the Internet

can see what components are being ordered, and with rapid systems retooling adjust their schedules appropriately—on the fly, if necessary. With the information flowing, the various players can ensure the desired components are at the production line when that customer's order is being assembled, whether it's a car or a three-piece suit. Customers order a car or a suit or anything else, specify the desired components, and have it built or assembled as ordered. Daihatsu Motor Company is already using 3D printers to offer its car buyers 10 colors and 15 base patterns to create their own "effect skins" for the car exterior. Each order rolls off the assembly line customized to that individual buyer. And it's no big deal. With IoT, mass customization is starting to happen.

Now imagine what's possible when you can connect anything with anything—production lines with parts and components, production lines with suppliers, products with service providers, logistics operations with transportation companies—and you can do it in near–real time. Designers could create products people really want and use, marketers could sell those products the way people want them, and service and support teams

would know where potential problems are and address them before things break. Costs could be contained, and customer satisfaction would soar.

Or imagine if products you put out in the field could link back to you, signaling when a part starts to fail or a configuration isn't working correctly. You could effectively eliminate unplanned downtime. What could product managers do when they learned that customers were using the company's product in new ways the marketing teams didn't even imagine? The possibilities and opportunities are endless. Admittedly, not all of these concepts and value propositions are available at scale today, but there are plenty of mature, fast paybacks you can implement now.

At the same time, there is no magic here. That's right; *no* magic is at play, none, nada. We're talking about the same digitally connected world we know now, just more so. Essentially, we're using the cloud as we know it, plus an intelligent infrastructure within which every device is digitized and addressable over a common IP network. Yes, there are a few new innovations—such as fog computing, a form of cloud computing at the edge of the network for real-time data processing; blockchain technology, essentially a secure distributed log; and machine learning, the technology behind real-time predictive analytics—but none of these is magic either. These are concepts that industry is focusing on and implementing (if you can't wait to learn more about them, we will cover them in more detail in Chapter 10); nothing exotic, nothing magical.

IoT Background—A Brief History

For many people, the first time they heard about IoT was in the business media or at a business conference. But IoT isn't actually new. It has been around for years, in various forms. Banks run large, distributed automated teller machine (ATM) networks. Retailers operate large point-of-sale (POS) networks, as well as extensive deployments of radio-frequency identification (RFID) tags to track the movement of millions of inventory items. Manufacturers connect thousands of devices to monitor and manage production in machine-to-machine (M2M) networks. Utilities deploy connected sensors and meters to enable everything from customer billing to maintenance troubleshooting. Each network could amount to tens of thousands of connected devices.

Nobody referred to these initial networks as IoT, and there were significant differences. Typically, they dealt with only one type of connected device or one application, had a very limited and tightly defined set of functions, and often used proprietary protocols rather than IP or the cloud, which have become the dominant networking and computing options today. Still, these amounted to early large-scale attempts to connect devices with some level of built-in intelligence and communication for the purpose of managing critical business functions. They were the forerunners of what we think of as IoT today. As expected, not all initial IoT-driven efforts were successful. From the GE-Cisco Industrial Ethernet joint venture, to location-based digital advertising platforms, to active RFID implementations in retail, and to ambitious plans for smart cities, many concepts incubated in the early 2000s were for one reason or another ahead of their time. However, as IoT matured over the following decade, the more robust technologies, solutions, and business models were subsequently developed and increasingly adopted.

As I recall, an IoT term might have been coined in late 1990s to describe the emerging RFID networks. To be honest, six years ago, when Cisco was deciding how to best describe the trend of devices, machines, or things connecting to each other over the IP networks and, ultimately, to the Internet, it chose not to invent a new term. Cisco simply decided to adopt the original Internet of Things idea and apply it to the phenomenon we were seeing at the time. In effect, we morphed the IoT of yesterday to define the IoT of today—the next stage of the Internet.

The first generation of Internet adopters also didn't use the term IoT to describe the type of business transformations that are taking place now. Then, as I said, about six years ago things began to accelerate on the network connectivity front. The first stage of the Internet was in full swing, driven by the rise of cloud computing and the growing adoption of smartphones and tablets with the goal of enabling us to connect to each other, to the data, to the processes, and to the services we were using. The devices, however, were already pointing the way to the second stage of the Internet—the IoT we see emerging today.

We now have a robust standards-based global networking infrastructure and a myriad of connected devices from all sorts of sensors, meters, actuators, to cars, buses, robots, drills, MRI machines, office buildings, entire cities, even garbage cans—those assets can not only communicate

but also generate and often process data and interface with a mind-boggling array of applications. And people have begun to adopt IoT terminology to recognize this phenomenon, the breadth of its scope and capabilities. IoT today is becoming pervasive.

You can clearly see a transformative power of IoT in the auto industry. Have you bought a new car lately? Well, the car is becoming a smartphone on wheels. Cars have long collected data from standalone subsystems and used processors embedded at various points to monitor and manage different functions. Car manufacturers are now installing standards-based high speed deterministic networks to connect all of these subsystems, the data they produce, and processing power into what amounts to a mobile datacenter. They're also connecting these mobile datacenters to the Internet. Pretty soon, every new car will be both smart and connected.

Remember when you bought a car based on its style or maybe key specs such as horsepower or its miles-per-gallon (MPG) rating? If you haven't bought a new car lately, your current car—I hate to tell you—is a dinosaur plodding along a path to extinction. If a car lacks even a Bluetooth interface, its trade-in value will be considerably lower. Car-buying criteria have changed completely for the majority of buyers. The electronics and device connectivity make a car appealing today. Similar changes are sweeping other industries. And it's due to the rise of IoT.

Now when we purchase a new car, we're actually buying, as I noted, a smartphone on wheels (Figure 1.4) and a mobile datacenter. Looks and style are important, of course, but for the majority of us speed and performance are secondary. What we really care about is how we interact with the car and how we automate tasks. We also care about how the car interacts with us—telling us when to change the oil based not on the mileage but on the actual use of oil. The car should warn us, and the dealer, that a part in the engine is about to break before it happens. And in the next few years we should expect an electric car to just pick us up and drive us wherever we want to go. Everything else becomes an afterthought.

Asit Goel, senior vice president and general manager at NXP Semiconductors, responsible for the firm's IOT solutions, summarized this new world well: "Ultimately, technology needs to replace or augment the

Figure 1.4 Smartphone on Wheels

senses of a human driver in a smart connected car. An army of sensors, radars, laser scanners, cameras, computing processors, wireless and cellular communications devices is needed to do this, to gain a 360-degree view of the car's surroundings and make critical decisions. The car isn't just a thing anymore; it's a system of things that delivers this hyper-connected experience with greater fluidity of service across my personal device, professional environments, and more."

Is the auto industry ready for such a dramatic transformation? Ford Motor Company's James Buczkowski, a Henry Ford Technical Fellow and director, Electrical and Electronics Systems Research and Advanced Engineering, has emerged as a thought leader on automotive electronics, including connected and autonomous vehicles. He assured me that the industry is comprehensively addressing smart mobility, which includes user experience, software, cyber security, data analytics and working toward new emerging mobility business models.

IoT Today—Digitally Transforming the World

Did the previous discussion about smart cars leave you disconcerted? Don't be. It's just the latest example of the revolution sweeping the world—and with it every industry segment. This new stage is transforming everything from the local pizza shop in Germany to a global Fortune 500 company in the United States; from an ice cream shop in India to brand new cities in China and Korea; from water pumps in Africa to wind farms in Europe. Businesses, governments, and nongoernment organizations are scrambling to figure out how they must adapt to thrive in this new world. That's the attraction—and payoff—of IoT.

So is adoption of IoT optional? Can you skip it or ignore it? For a while yes, but at considerable risk. Think of the horse and buggy industry at the start of the 20th century. The buggy and carriage trade survived for a couple of decades. Today it exists only for a few collectors and specialized use cases.

IoT is producing an economic tidal wave that will engulf everything in its path. Tim Jennings, chief research officer at Ovum, an analyst and consultancy firm that publishes the Machine-to-Machine and Internet-of-Things Contracts Tracker, told me that IoT is being adopted across many industries. Manufacturing, business services, and energy and utilities sectors are leading the way with most IoT deployments to date, with transportation, retail and wholesale, public sector, and health care industries being next in line. "As digital transformation accelerates across industry sectors, permeating deeper into the enterprise, the Internet of Things has become a key enabler of digital operations, with Ovum's research showing that deployment is occurring across a wide range of connected business processes," he commented. "An initial wave of adoption tended to focus on industry-specific use cases, but we are now seeing the emergence of cross-industry applications built on IoT platforms. Coupled with increased business awareness, we expect enterprises to take a more systematic approach to digitizing their processes and operations, and look for new opportunities to create business value from the Internet of Things," Jennings added.

We've already peeked at IoT in factories through Harley-Davidson. This book will also discuss other industries, focusing primarily on the B2B segment since B2B innovations are driving the transition to IoT today.

Moving forward, the research conducted by James Manyika and Michael Chui of the McKinsey Global Institute in July 2015 pegged the real dollar value of the global IoT market at potentially $11.1 trillion by 2025.[3]

Will this economic tidal wave hit your industry? Without a doubt. It will hit every industry and every segment sooner or later. McKinsey projected the first nine impacted industry segments as seen in Figure 1.5.

Ovum and McKinsey, of course, are not the only observers to weigh in with IoT status and projections. In May 2016, IDC's Vernon Turner predicted that the worldwide Internet of Things (IoT) market spending will grow from $692.6 billion in 2015 to $1.46 trillion in 2020 with a compound annual growth rate (CAGR) of 16.1 percent.[4] Furthermore, "We expect the installed base of IoT endpoints to grow from 12.1 billion in 2015 to more than 30 billion in 2020,"[5] Turner told me. In a July 2014 report titled "Hype Cycle for Emerging Technologies, 2014" written by Hung LeHong, Jackie Fenn, and Rand Leeb-du Toit, research and advisory firm Gartner put IoT at the top of the "hype curve,"[6] Gartner's terms for the blizzard of vendor hype that accompanies technology advances. Going forward, we can hope that the hype will start to subside as organizations embark on substantive IoT initiatives.

Why Now: Three Driving Trends

As previously noted, IoT isn't exactly new, having been around in different forms for more than a decade (think RFID, where every item sold at a retail store can speak with the supply chain). So why is it finally generating so much attention? I see three major trends coming into play:

- **The lines of business, as represented by the line of business (LOB) manager, are emerging as a major buying center for technology.** LOB managers are concerned with business outcomes and look for business solutions, especially those that reduce cost, increase productivity, and—most importantly—increase profitability. They look for the ways to improve overall equipment effectiveness, production delivery times and throughput, asset uptime and increasingly target specific sustainability metrics. Line of business managers weren't among the primary beneficiaries of the first stage of the

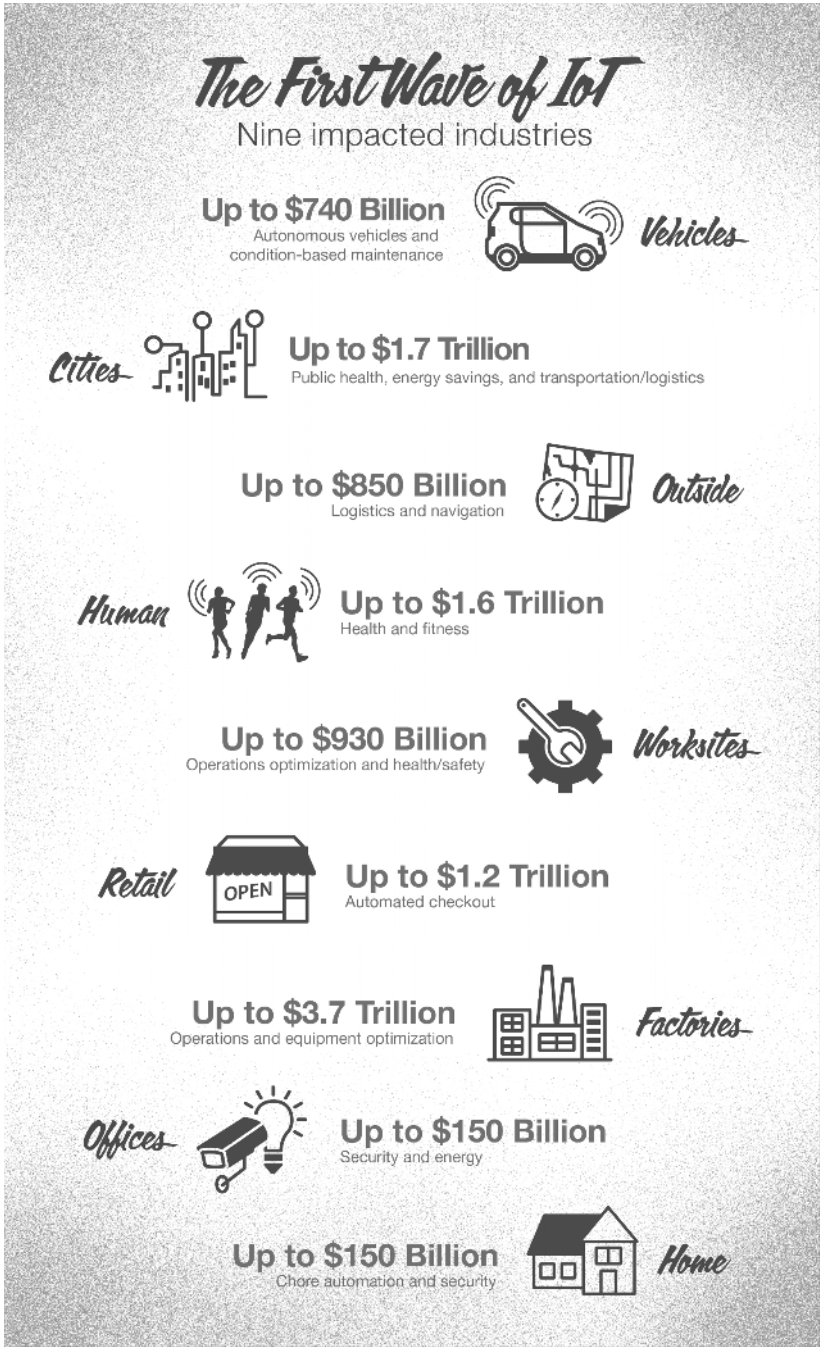

Figure 1.5 McKinsey Projection of Impacted Industry Segments

Internet, which focused on IT, service providers, and consumers. Today, however, LOB leaders are starting to harness technology to drive business outcomes. As a consequence, unlike the Internet's first stage, IoT promises not to be a technology-led transition; rather, it's a business-driven transition where technology is a tool to achieve specific business goals. Yes, LOB managers can create and spend budgets, but they're looking to increase both top-line and bottom-line results. For example, some manufacturing operations are reporting a 160 percent return on investment (ROI), a 20 percent reduction in cost, and a 75 percent reduction in network downtime from IoT. To LOB managers, such outcomes demonstrate a value proposition so compelling that they're willing to open up their wallets to fund such efforts.

- **The convergence of information technology and operational technology improving communication and efficiency.** Remember when millions of people read John Gray's book *Men Are from Mars, Women Are from Venus*? This best-seller suggested that the frequent misunderstandings between genders make it seem as though men and women are from different, alien worlds. But it's not just men and women who appear to be from different planets. Today, every organization that has begun an IoT deployment is bumping up against a fundamental disconnect between IT and OT. In many cases, these two groups are "alien" to one another—they have separate technology stacks, network architectures, protocols, standards, governance models, and organizations. IT/OT convergence is the solution, yet it didn't begin to happen until recently. Perhaps it takes a prolonged downturn, followed by a lackluster recovery, to make this happen. Alternatively, maybe the emergence of IoT multiplies the networked connections among people, processes, data, and things to the extent that it compels the worlds of IT and OT to converge out of necessity. The key driver, however (as shown in powerful use cases we will discuss later in this book), is the need for the data to flow between plants, enterprise infrastructure, and the cloud.

  Such a need forces IT/OT convergence at the technological, architectural, and organizational levels. Of course, with this convergence comes a culture clash. Each organization has a long litany of complaints against the other. And each has completely valid concerns, all of which have to be resolved quickly. (As we mentioned, Harley-Davidson's solution to this challenge was to put representatives from both teams together in a room and not let them leave until all of their issues were resolved.) Despite the potential for a culture clash, over the past decade or so, OT and LOB functions have increasingly

adopted IT-like technologies, such as Ethernet/IP and even cloud services. A 2014 Cisco study by Andy Noronha, Robert Moriarty, Kathy O'Connell, and Nicola Villa titled "Attaining IoT Value: How to Move from Connecting Things to Capturing Insights" found that both IT and OT leaders now recognize the need to share responsibility for IoT solutions, although they may still need to negotiate decision-making authority over each stage in the adoption process.[7] It also helps that increasingly IT organizations report to the LOBs, further aligning the technology and business agendas across the enterprise.

- **The proprietary/specialized technologies moving to open standards.** In the last two decades of the 20th century, the manufacturing industry went through the so called fieldbus wars, where several camps of vendors fought to establish their proprietary technologies as de facto communication or security standards for the industry. In the aftermath, a bunch of overlapping semi-standard technologies (including proprietary extension to open standards) was embedded into products locking customers into specific sets of vendors. Thus, despite the initial good intentions, the industry further diverged from common standards. Add to that a large number of existing single-purpose specialized or proprietary legacy protocols and the result was chaos, higher costs, little innovation, and Balkanized market. Since then, however, an increased number of vendors started to embrace standard and unmodified Ethernet and IP technologies and integrate them into their offerings. Today, most of the end-devices have Ethernet interfaces and the momentum is mounting to establish common truly open standards in the industry. We see the same transition starting to happen in other markets too, from transportation to healthcare to retail. The customers are increasingly demanding open standards and interoperability. In addition, the IT and OT vendors are joining forces to evolve existing horizontal standards to address the OT needs and are adopting open standards in vertical standards bodies and consortia. According to the Cisco report cited earlier, by year 2020, there will be as many as 50 billion connected devices.[8] Whether the actual number ends up being 50 billion, 30 billion, or even 7 billion, these are still staggering figures. Not long ago, on a typical manufacturing floor, there were just a few connected devices for every engineer; now there are dozens of these devices and soon there may be hundreds of them per every person working there. Converging all of these devices on one open unified standards-based network is not only a cost-effective and scalable way to get them connected but also a key to unlocking the revenue potential of IoT.

This book will discuss these three trends, as well as new value propositions such as connected operations, remote operations, predictive analytics and preventive maintenance. Because IoT is still a nascent discipline, industry segments have only begun to address related issues in the last few years.

A "Perfect Storm" of Technology, the Economy, and Culture

IoT is bringing together three key elements—technology, the economy, and culture—to form what can be popularly described as a "perfect storm." Whereas a lethal brew of elements is typically associated with a dangerous storm, IoT's wide open opportunities can be embraced by any organization that wants to be involved. In the process, we're all experiencing a massive rebalancing of key economic, social, environmental, and privacy/security priorities. Although the landscape is full of "900-pound gorillas," none has succeeded in dominating this issue. (Full disclosure: My own organization, Cisco, aspires to be an influential IoT leader.)

The truth is IoT presents an opportunity for every organization, not just a few chosen companies. Even small and midsize enterprises can participate. Winners will transform their businesses based on open standards and build ecosystems of partners to deliver vertical solutions based on horizontal capabilities. Meanwhile, losers will ignore these changes and stick to their old business models based on proprietary or semi-proprietary technology and ensure customer lock-in until those customers steadily abandon them. (With luck, some of these companies will realize the problem before it's too late. Others, sadly, never will. Remember the changes to the make-up of the S&P 500 over the past decades?)

In terms of *technology,* IoT is adopting cloud-oriented technology even as it drives an architecture shift to fog computing as an extension of the cloud to the edge. At the same time, IPv6-driven networking and nimble open technologies have been driving the corresponding application explosion. Fog computing, meanwhile, is removing latency and enabling real-time analytics and responsiveness while Time Sensitive Networking is offering real-time guaranteed latency for time critical traffic. Very quickly, you will see new technologies evolve to clearly distinguish IoT

as the next stage of the Internet. I call them IoT-native technologies and applications—designed and optimized around everything connecting to everything.

With regard to *the economy,* the compelling benefits of IoT are leading LOB managers to welcome it. The expected result is a multi-trillion-dollar boost to the economy before the end of the decade.

As for *culture*, the opening of communications and collaboration between OT and IT as an extension of the popular DevOps trend, as well as the rise of LOB managers, highlight the changes underway.

There you have it: technology, the economy, and culture all coming together in a perfect storm that will do good things for those organizations open to change. Like every big storm, however, IoT will create dramatic impact—in this case, a massive rebalancing throughout the economy. Some of the early winners are already emerging, among them:

- Flexible business managers and LOB leaders, who can envision new business models and lead their organizations to new opportunities that arise when everything can communicate with everything. They must also be prepared to fully leverage the data, automation, and analytics that are key to capitalizing on IoT.
- Application developers and programmers, who will be in high demand as IoT brings about the API economy that will consume millions of apps, digital containers, and micro-services. IoT will also require large numbers of data scientists, data managers, and data analysts to create, deploy, manage, and leverage the automated data analytics that must make sense of and handle the massive volume of data as it's generated, collected, analyzed, or acted upon.
- Some economic sectors will experience a renaissance. Manufacturing and the rest of the "maker" movement is already an early beneficiary; for the first time in generations, young people—popularly referred to as Millennials—are being attracted to manufacturing. Never believed I'd actually write this: Manufacturing is cool again. Add to this 3D printing, drones, and all manner of new materials and network-connectable electronics and you start to get a picture. Other industries, such as business services, energy, utilities, transportation, retail, wholesale, public sector, and health care, will stand to gain big from IoT as well.
- Automation and analytics users are clear winners. The scale and volume of information creation and distribution requires automation and real-time analytics. People will set up the algorithms and rules, and then automation will have to take over. You can't operate fast enough

at this scale manually. As IoT ramps up, people will need to be aided by automation and analytics if they're to have any hope of keeping up with the volumes.

- New industries and opportunities, including real-time remote operations, smart (connected) cities and communities, and analytics-driven real-time security are all emerging.

The world after this perfect storm will be IoT-native, mobile-connected, automated, and driven by smart analytics. It will be real time, API-enabled, open, security-focused, and built around micro-services that can change virtually on demand.

Key Obstacles

This isn't meant to imply that IoT is inevitable and doesn't face hurdles. To the contrary, it faces significant obstacles in four broad areas: technical, security, organizational, and government.

- *Technical (privacy, standards/interoperability).* To deliver on its promise, IoT needs to assure privacy, the variety of connected devices needs to operate and interoperate seamlessly, and data needs to be exchanged in a fluid and understandable way. All of this requires truly open standards, industry-wide interoperability, and universal adoption of industry-accepted protocols. The traditional IT and OT standards groups are already tackling these problems, while new consortia are being created and old ones are being refocused. Semi-proprietary "standards" are starting to give way to those that are truly open. The industry knows how to do it; we did it for the first stage of the Internet and for the cloud. The current task at hand is even bigger and more complex, but the I know that the IoT community is up for the challenge.
- *Security.* To paraphrase real estate industry wisdom about the importance of location, IoT requires ironclad security, security, and security that management and users can count on. Many of the security components exist today, and many can be leveraged by extending current IT security architectures to OT. Plus, many new use cases such as vehicle-to-vehicle identity requirements, sensor swarms, always-on systems, and smart security paradigms are being addressed by the waves of new IoT security startups, academia, and established vendors. Companies like Harley-Davidson are deploying IoT without

undue risk. However, more must be done not only to reduce the number of security breaches but also to enable the early detection of cyber attacks and to minimize their impact on businesses while protecting the privacy of individuals. Equally important, self-reliant systems and devices that can continue to safely function even if under attack must be deployed. Smart analytics being built into IoT, especially with fog computing designed to deliver real-time processing, will go far in addressing a number of security gaps.

- *Organizational (cultural change).* This may be the biggest obstacle. Change is hard, especially for established organizations that, for decades, have been so successful with their existing business models, practices, and processes. It isn't easy for IT and OT to come together and cooperate, and it isn't easy for vendors to embrace common open standards but it has been done; the benefits are undeniable. Change is mostly a question of communication, leadership, retraining, and keeping an open mind. Opportunities as large as IoT provide a strong incentive for everyone to cooperate.
- *Government.* IoT benefits government in the form of smarter cities, like Barcelona, Spain, arguably one of the most advanced smart cities on the planet today. But in addition to adoption, government also has a role to play in regulating and agenda setting, ensuring that IoT develops and grows by applying regulations in some areas but also easing regulatory impediments in others to encourage new business models based on IoT.

These obstacles are far from insurmountable. Technical groups and industry and advocacy organizations are already working in various areas, hammering out standards and identifying best practices. Key components, similarly, are falling into place—from IP to cloud and fog computing to application development environments and real-time analytics. The common elements of IoT solutions, even at this early stage of maturity, reach across most industries and are being deployed by thousands of customers worldwide.

Scope of the Book

As noted above, I've traveled endless miles while meeting with business managers and discussing with them their challenges and questions about IoT. I wrote this book to help managers at midsize and large organizations

understand what IoT is really about, why they need to adopt it for their businesses, and how they should go about doing this—specifically, how to start on an IoT journey. There is no reason, however, that smaller organizations can't fully participate in IoT; they already take advantage of cloud computing, IP networking, analytics, and the other core components of IoT. The book's focus on predominantly midsize and large organizations is the result of my personal IoT experience, which comes from that specific environment. However, a combination of the above core components, mature and proven fast payback use cases, and well-established integration channels should allow smaller organizations to fully embrace IoT, just as they embraced the Internet and the cloud.

Similarly, the book will primarily focus on B2B opportunities, with some B2B2C activity. IoT has a significant business-to-consumer component today, but that mostly falls outside the scope of this book. In the same way, this book will draw from key major vertical segments—primarily manufacturing, oil and gas, transportation and logistics, utilities, and government. It will also touch on retail, health care, agriculture, education, finance, and specialized situations like the connected car.

By reading this book, you've already started on the road to IoT. Figure 1.6 shows a recipe for IoT success. If there is one thing you take away from this book, this recipe is it. It summarizes what I believe are fundamental elements you should internalize and operationalize in order to effectively plan and implement your IoT efforts. I will elaborate on these eight points throughout the book.

In the meantime, if you're just taking a first step in your IoT journey, here are a few tips to begin:

- Begin talking about IoT in your organization, help people think about what might be possible when things can communicate with other things.
- Identify some operational and strategic goals for your IoT initiative—identify a problem to solve or an opportunity to grab. Have a big vision, but start small with low-hanging-fruit scenario.
- Introduce OT and IT team members and get them talking.
- Identify and secure a C-suite sponsor for your IoT efforts.

With IoT, you're embarking on a journey to the future. That certainly was the experience at Stanley Black & Decker, Inc., another early

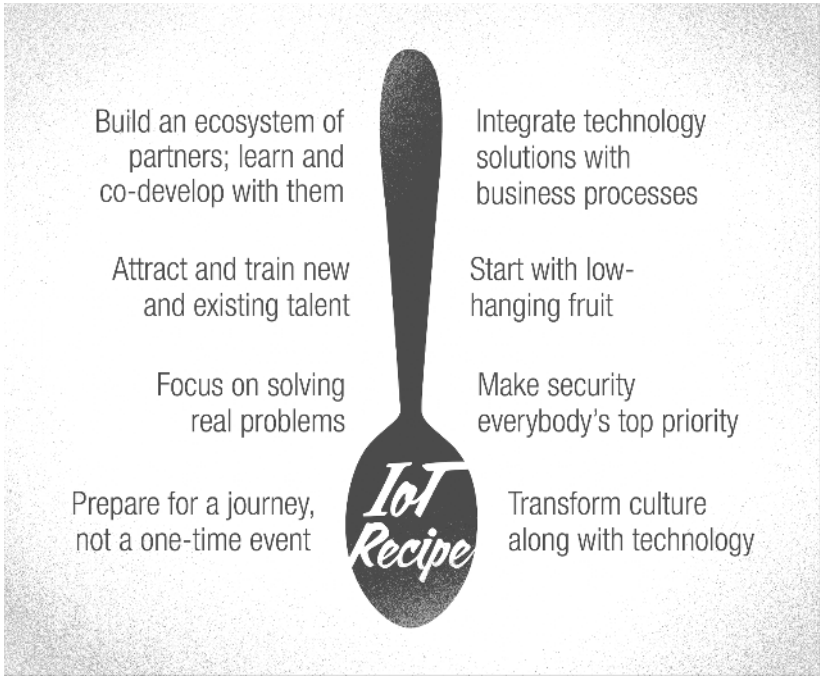

Figure 1.6 Recipe for IoT Success

IoT adopter. "We are on our way toward realizing our vision of a virtual warehouse and fully connected factory, with complete visibility and traceability," said a C-level executive at the manufacturer. Complete visibility and traceability. Would some version of that appeal to your organization? There's no reason it can't apply to your business, too.

How to Read This Book

Not every reader may feel the urge to read this book cover to cover. You are welcome to jump around following your particular interests and concerns and come back to a section that addresses a particular challenge you are currently facing. Use the following brief chapter descriptions as your guide.

Chapter 1, as you have just discovered, is an overview of what this book is about and introduces some of the basic concepts.

Chapter 2 looks at IoT adoption and puts the astounding growth projections into a meaningful perspective.

Chapters 3 and 4 address new business models and the business value proposition.

Chapter 5 provides a number of fast payback IoT models for readers who want to immediately start to benefit from IoT.

Chapter 6 explores the ways IoT impacts careers and workplace roles.

Chapter 7 looks at how IoT will change your organization.

Chapter 8 recognizes that IoT doesn't always deliver as promised and looks at common pitfalls and mistakes.

Chapter 9 provides an overview of the IoT security challenge and how it is being addressed.

Chapter 10 provides a similar overview of IoT standards and technology directions, the emergence of open IoT architectures, and ways to overcome integration issues.

Chapter 11 summarizes current state of the union of IoT, my vision of where IoT is going in the next 10 years and how you, the reader, can play a key role in charting the IoT future in your organization.

The next chapter discusses business change and transformation, which is what IoT is really about. It also looks at some quick paybacks—focusing on the low-hanging fruit—and some early success stories. OK, let's get started on your IoT journey.