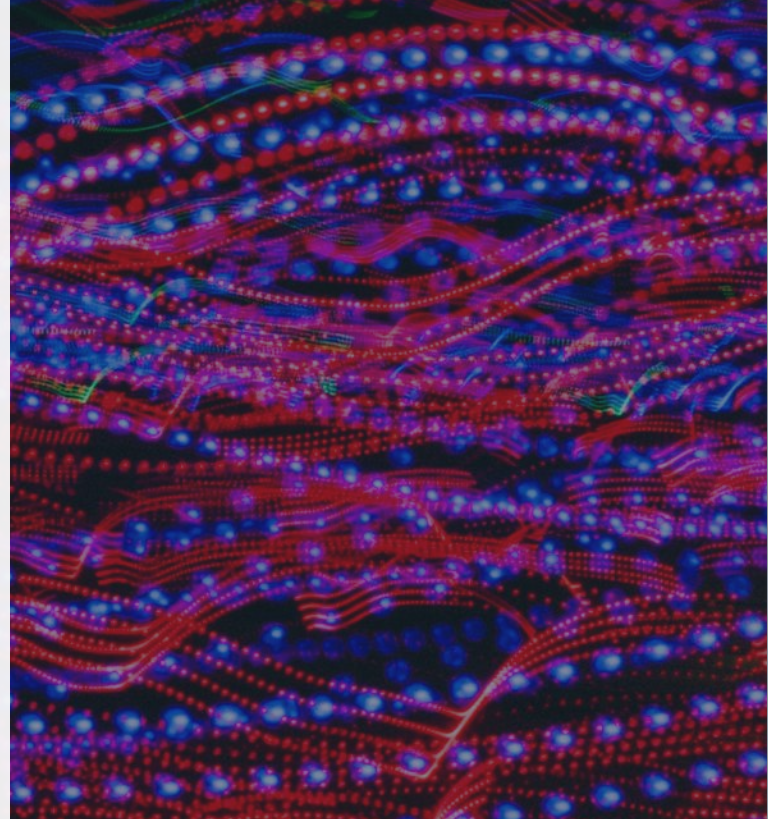


INTERNET OF THINGS 2017

EXAMINING HOW THE IoT IS AUGMENTING
WORKPLACES AND LIVES TO TRANSFORM
THE WORLD

January 2017

Peter Newman | Research Analyst



BI INTELLIGENCE

KEY POINTS

- **The Internet of Things (IoT) is a growing network of connected objects able to collect and share data via embedded sensors.** The proliferation of these devices is upending traditional practices through the introduction of data analytics and automation, and transforming the way people and groups interact with the world.
- **The IoT ecosystem has five distinct components.** Any IoT implementation, whether in a manufacturing plant, a connected car, or a smart home, will use:
 - **Hardware**, or the devices within the IoT solution.
 - **Networks** that connect the IoT solution to the user.
 - **Remotes**, which provide the user with an interface to connect to and manage the IoT solution.
 - **Platforms** that provide messaging, analytics, and data storage components.
 - **Security protocols** that ensure the IoT solution remains protected.
- **BI Intelligence projects that in 2021, the number of IoT devices installed will rise to 22.5 billion, up from 6.6 billion today.** This growth will lead to major increases in efficiency and productivity, as companies and platforms discover innovative new means of using the devices they put in place and the data those devices produce.
- **Companies implementing the IoT are focusing on smaller device installations.** At companies that have or are in the process of implementing IoT solutions, 51% of respondents say their companies will use fewer than 50 IoT devices, according to exclusive BI Intelligence data. Large scale implementations (1,000 devices or more) are generally limited to companies with over 500 employees.
- **We estimate that annual spending on the IoT will rise from just under \$400 billion in 2016 to \$1.35 trillion in 2021.** This estimate is based on device projections, platform costs and growth projections, and data on device operation and associated costs. **In total, we expect \$4.8 trillion in IoT spending over the next five years.**
- **The majority of companies surveyed by BI Intelligence will invest less than \$100,000 in IoT implementations,** with 25% of respondents investing between \$1,000 and \$25,000, and 27% spending between \$25,001 and \$100,000. The increases in overall investment in the IoT in the years ahead will come from the multitude of companies pursuing these implementations.

- **IoT deployments can be broken down into five separate and distinct stages: connecting devices, managing devices, analyzing device data, creating interoperability between devices, and automating devices.** Interoperability and automation are the most difficult to attain, with only 17% and 16% of our survey respondents, respectively, saying they've reached these stages. This will likely change in the years ahead as the technology that powers the IoT matures.
- **The market is largely driven by the technological innovations of the providers that create, implement, and maintain IoT solutions.** IoT providers must develop services and products that appeal to potential users, assuage their concerns, and provide them with value to justify potentially substantial investments. Although this leads to challenges, many of these companies have been involved in the IoT for longer than the customers they serve, affording them the ability to take their time in building out market-ready solutions.
- **IoT providers target three broad groups of IoT end users: consumers, governments, and enterprises.** Each uses IoT solutions in varying ways and offers different returns for these providers.
 - **Enterprise is the most targeted group by IoT solution providers.** The enterprise space is the largest potential market for providers, and should continue to see rapid adoption of IoT solutions in the years ahead.
 - **Governmental organizations, including cities, education, and defense, are less targeted, but still have promise.** Such projects are less common than enterprise implementations but can also be large in scale.
 - **Consumer devices, including smart-home devices and wearables, are less targeted and don't offer the same growth potential as enterprise or government customers.** However, the consumer IoT market has long-term growth potential.
- **The IoT will further make its way into the mainstream of corporate, industrial, and consumer culture in 2017.** As companies throughout the world continue to seek out, pilot, and fully implement IoT solutions, the total number of IoT devices will reach 8.4 billion in 2017.

[Download the charts and data in Excel »](#)

INTRODUCTION

The Internet of Things (IoT) is a growing network of connected objects able to collect and share data via embedded sensors. In the past couple of years, the IoT has reached the mainstream among businesses and become a central part of consumer mindspace. More and more people, businesses, and organizations are connecting devices, using sensors to gather data from them, and using that data. This confluence of technologies is changing the way these people and groups interact with the world.

BI Intelligence projects the number of IoT devices installed will rise to 22.5 billion by 2021, up from 6.6 billion today, and that cumulative investment will top \$4.8 trillion. Connected to the internet and equipped with sensors, these devices power much of the developing data-based economy and bridge the divide between the physical and digital worlds. They are part of a broader ecosystem that also includes the networks that connect them, the remotes that allow users to manage them, the platforms that facilitates analysis and storage of the data they generate, and the security protocols that protect them from malicious interference.

Taken as a whole, this ecosystem provides enterprises, individuals, and governments using the IoT with the ability capture and interpret actionable data about their factories, homes and cities and fully leverage the potential of a connected world.

Many of the key insights in this report come from BI Intelligence's Global IoT Executive Survey, which was conducted in the third and fourth quarter of last year. For more information on how the survey was conducted, please see the "Survey Methodology" section at the end of this report.

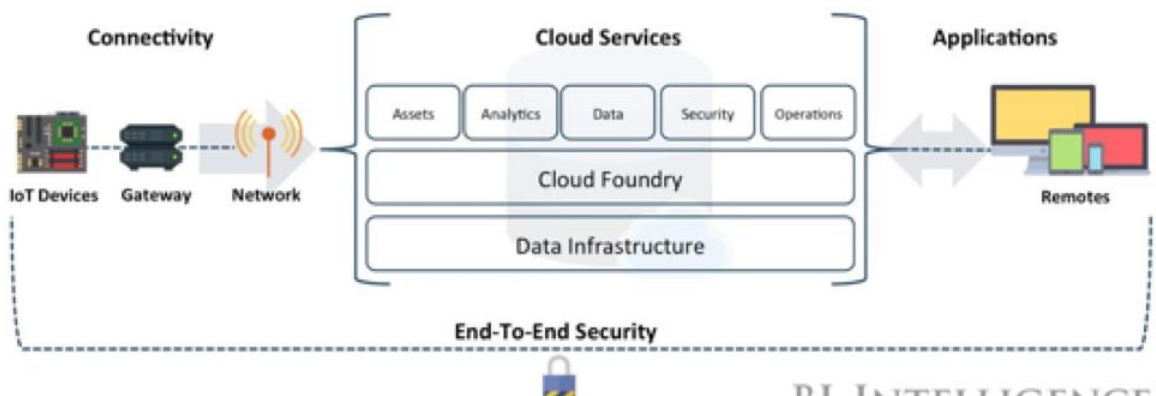
In this report, BI Intelligence details the components that make up IoT ecosystem. We size the IoT market in terms of device installations and investment through 2021. And we examine the importance of IoT providers, the challenges they face, and what they do with the data they collect. Finally, we take a look at the opportunities, challenges, and barriers related to mass adoption of IoT devices among consumers, governments, and enterprises.

THE IoT ECOSYSTEM

The IoT ecosystem consists of the software, hardware, and networking technology necessary for end users to use an IoT solution. It's made up of five distinct components:

- **Hardware**, or the IoT devices within the IoT solution.
- **Networks** that connect the IoT solution to the user.
- **Remotes**, which provide the user with an interface to connect to and manage the IoT solution.
- **Platforms** that provide messaging, analytics, and data storage components.
- **Security protocols** that ensure the IoT solution remains protected.

IoT Ecosystem



Source: Based off GE Predix graphic

BI INTELLIGENCE

This ecosystem is applicable to any IoT setup, regardless of the details of an implementation. Any solution, whether in a manufacturing plant, a connected car, or a smart home, will utilize hardware, a network, remotes, a platform, and security protocols. The industries utilizing the IoT include retail, healthcare, transportation, logistics, and more.

Hardware

The most basic purpose of the IoT is to add internet connectivity to nonconnected devices in order to gather actionable data about the environment that they inhabit and interact with. To add connectivity to devices in the home, car, city, workplace, or factory, though, requires specialized hardware. Microchips enable the computing that lets such "smart" devices communicate both with each other and with centralized platforms.

The rising prominence of the IoT has led to major transformations in the semiconductor industry, with leading companies in the microchip space adapting to capitalize on the IoT's rapid growth and increasing share of the silicon market. Semiconductor chips enable sensors to be attached to devices that can regulate data generation, transmission, and device activity.

Intel and ARM are the two biggest players in semiconductor design, and both are transforming their businesses due to changing consumer and client demands. Intel [incurred](#) \$1.4 billion in restructuring costs in the summer of 2016 as it transitioned its workforce to focus on cloud and IoT development instead of its traditional PC market sector. And it's shifted part of its semiconductor development [away](#) from traditional microchips and toward those aimed at embedded and mobile devices that are used in the IoT. This has also led to an emphasis on low-powered microchips throughout Intel's lineup of offerings.

The IoT demands a different sort of processor, and its increasingly prominent role has forced semiconductor-market leader Intel to invest billions of dollars to meet new and projected demands. IoT devices don't need the versatility of powerful, electricity-hungry processors like PCs; instead they require low-powered processors that fulfill a few specified functions. Intel is working to transform a major part of its production to create these new types of microchips.

ARM, which Softbank [purchased](#) for \$32 billion in July 2016, is known primarily for its low-powered mobile chip designs, which are used in the vast majority of mobile phones and devices around the world. The company [projects](#) that microchip sales for embedded IoT devices for the home, the city, industry, and wearables will exceed \$8 billion in 2020, which has prompted it to transform its design team and shift some emphasis away from mobile and toward the IoT market. It is also transitioning to the server space, which goes hand-in-hand with an emphasis on IoT development, as IoT platforms are typically cloud-based and require chips optimized for data storage and processing to enable analytics.

What to watch for in 2017: As more devices are connected, the underlying semiconductor hardware will be increasingly important to the development of the IoT. Both Intel and ARM are refining microchip manufacturing techniques that will cut the price of embedded semiconductors to less than \$1 per unit, allowing for faster proliferation in the IoT in the year ahead. New, cheap, and low-powered hardware will foster increasingly rapid IoT growth.

Networks

Just as computing hardware is central to making devices smart, networks are critical to making these devices connected. IoT solutions and devices employ a variety of networks that enable the transmission of data to analysis platforms. Without these networks, there is no internet, only things.

IoT solutions can employ a variety of networking protocols to enable communication. Some of the most popular and widely used are:

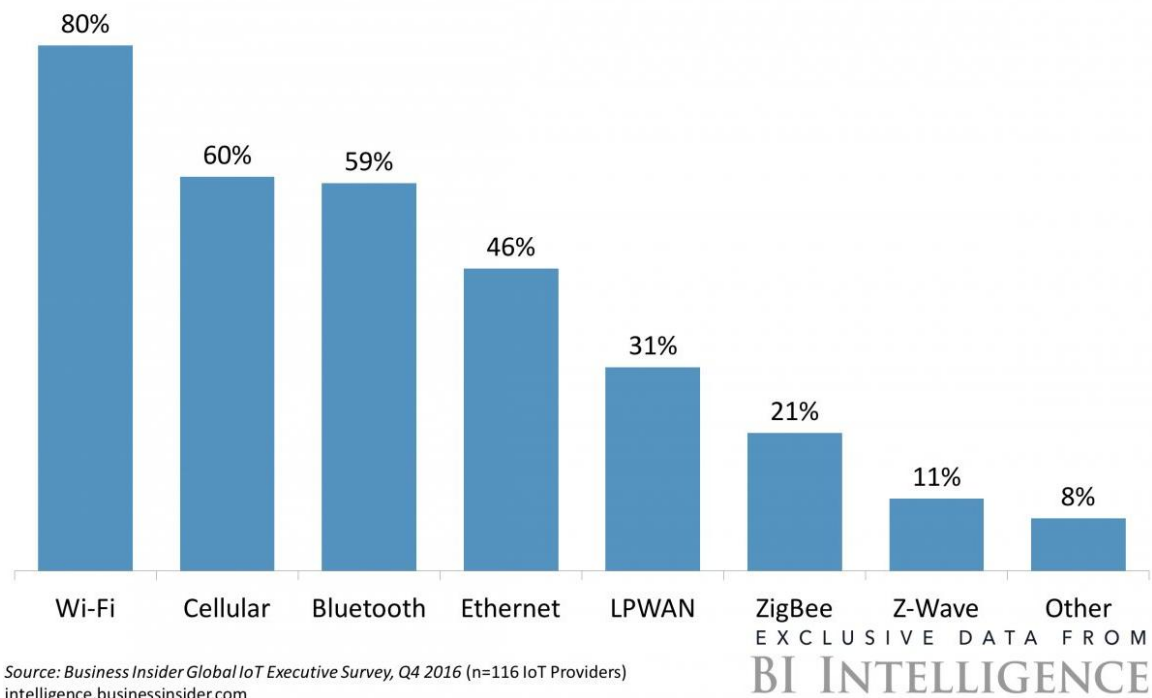
- **Wi-Fi/Ethernet:** The ubiquitous IP-based networking standard, it can be wired or wireless, with very high data rates over relatively short ranges. It is known and used by consumers as well as in enterprise and industrial use cases.
- **Mesh networks:** Multiple devices are connected to one another on a mesh network. Each device acts like a router, spreading data around for transmission to create multiple pathways to move data from device to server. This makes the network resilient even if some devices fail. Examples of mesh networks include Z-Wave, ZigBee, and Bluetooth.
- **Cellular:** Another widely used communication standard, cellular service can transmit at a variety of rates. The faster the cellular network (4G is the fastest and newest, followed by 3G and 2G), the more power that device will use, forcing users to weigh transmission speed against power draw and battery life.
- **Low-power, wide-area networks (LPWANs):** Specifically designed for IoT solutions, LPWANs are much like cellular networks but offer very low power usage for devices at the price of low rates of data transmission.

According to our exclusive BI Intelligence survey data, Wi-Fi is by far the most commonly used communication protocol, with 80% of respondents saying their solutions employ it. Bluetooth (59%) and cellular (60%) are also widely used, while more specialized mesh networks like ZigBee and Z-Wave are less popular. It appears that solution providers are looking to integrate into existing infrastructures, rather than adding additional complexity by utilizing newer networks, in order to ensure client success and satisfaction.

What to watch for in 2017: IoT solutions will increasingly use more traditional and widely available networking technologies like Wi-Fi, Ethernet, and cellular, rather than potentially more efficient but less well-known mesh networking solutions. This is because companies implementing the IoT are emphasizing continuity and simplicity of integration over absolute network fit. In addition, LPWAN infrastructure will continue to develop as the technology matures, though widespread use won't come in 2017. Development will continue on the 5G cellular standard, which promises high data transmission rates at low power usage.

Networks And Communication Technologies Providers Use In Their IoT Services

Global, 2016



Remotes

Remotes provide an interface for users to interact with their IoT solution. Examples of remotes are smartphones, tablets, laptops, desktops, ultrabooks, connected TVs, voice speakers, and smartwatches. The purpose of these devices is not to function as an IoT solution, though they may offer an IoT component as a secondary capability. For instance, a smartphone can provide its location to a platform just like a GPS tag, but users don't buy a smartphone for that express purpose. Understanding the use case of each remote helps a company better optimize its IoT solution. For example, providing a PC instead of a smartphone to a utilities worker in the field is inefficient and will detract from the value the IoT solution could provide.

In the enterprise market, laptops and desktops are the devices most commonly used as remotes by workers due to their high computing power. However, a recent Cisco [survey](#) of IT and business global leaders found that tablets and ultrabooks (lightweight laptops, which sometimes also integrate some tablet functionality) will replace laptops and desktops by 2020. Further, 19% of respondents indicated that they believe wearables will be the primary device their employees use in 2020.

The shift from laptops and desktops toward mobile devices highlights the increasing number of workers unattached to a specific workspace. And Apple's release of the more robust and powerful iPad Pro shows how remote-makers are reacting to this trend by releasing mobile products that are designed for enterprise use. In order for IoT solution providers to offer the best possible products, they will have to offer solutions that are mobile-compatible.

In the consumer space, smartphones are the most common remotes. Smartphones are lightweight, highly portable, have high computing power, and enable users to easily connect to and manage their IoT solution. By 2021, Ericsson [estimates](#) that there will be more than 6.3 billion smartphone subscriptions, up from 3.2 billion in 2015, meaning that there will be nearly as many smartphone subscriptions as there will be people in the world. Because of this prevalence and consumer market penetration, smartphones will be the top remote for the next five years in the connected-home market.

Voice remotes, like the Amazon Echo and Google Home, may also become staples of the connected-home in the years ahead. More than 46% of Echo owners have used their Echo to control their smart lights at least once, according to a recent Experian [survey](#). Further, 30% of Echo owners have used them to control their smart thermostat. Voice commands remove the clunky user interface often associated with smart-home applications.

For example, if a user wants to turn off their lights and lock their doors, they may need to use two separate mobile apps, as opposed to one voice command. **As the number of people using these systems climbs, so will the number of people using their voices to control devices.**

Such voice-controlled systems employ artificial intelligence (AI) to make interactions more interactive. Alexa, Google Assistant, and Apple's Siri enable consumers to interact with smart-home devices through voice commands, and are able to respond as well. As these assistants develop additional capabilities, they will likely move beyond conversation and into automation. The assistants will be able to observe users' actions and commands, use them to deduce preferences, and then change settings autonomously.

What to watch for in 2017: Many executives in the smart-home industry expect the remote to eventually disappear as increasingly capable AI enables homes to react to their surroundings. For example, instead of responding to a voice command or directive from a mobile device, smart-home systems will eventually learn when inhabitants go to bed, and then turn off the lights and lock the doors on their own. Over the next year, AI as a remote will likely have an increasingly important role in not only the smart-home market, but all IoT environments. However, remotes will persist in the workplace to provide continued monitoring of processes.

Platforms

The term "IoT platform" has typically referred to the middleware that transmits messages between devices and data storage — in other words, the glue that holds the IoT together. However, the definition of an IoT platform has been expanded of late to include multiple components of the IoT including data storage, analytics, and in some cases, data communication and visualization. For example, an IoT platform provider may provide a middleware service that connects their data storage and analytics components, but choose to bundle the components together under the term "platform" because it makes it easier to package multiple services. As a result, many platforms are modular, meaning different components of a company's IoT platform can be used with those of other companies to ensure that a customer is getting the best service.

Many IoT platform companies have seen excellent growth over the last few years. For example, PTC's IoT Group, including the ThingWorx IoT platform, [generated](#) \$53 million in 2015, up from \$5 million a year earlier. Similarly, GE, which runs the Predix platform, generated \$5 billion from its analytical applications and software business in 2015, and realized \$500 million in productivity gains.

As a result of the growth of the IoT, many cloud providers have opened up software development kits to enable IoT devices to be easily integrated into their cloud platforms. The cloud providers charge per device, or per number of messages sent through their platform. For example, Amazon charges \$5 to \$8 per million messages sent, depending on the region. The more devices connected, and the more active they are, the higher the rates will become.

What to watch for in 2017: Many players in the IoT platform space are trying to build a full-stack offering, which means they're trying to offer all of the software components needed for an IoT solution. There are two ways companies can achieve this: investing in their IoT solutions and building new business offerings, or through acquisitions. For example, in September 2016, SAP acquired [PLAT.ONE](#) and [Fedem Technologies](#), while Cisco [acquired](#) Jasper technologies earlier in the year. In addition, the market is quickly becoming overcrowded with startups trying to provide components that help optimize IoT platforms. As these platforms become more robust and their technology is proven, they will likely be acquired and integrated into existing larger platforms.

Security

A major topic of conversation within the IoT over the past year has been the security of connected devices and the data they generate, with numerous news stories highlighting the difficulty of safeguarding them from hacking. Much of this news revolved around smart-home devices, such as a finding that the vast majority of smart locks tested [failed](#) to hold up against attempted hacks. In another instance, researchers [demonstrated](#) the ease with which hackers could infect a smart thermostat with ransomware.

Security issues were [headlined](#) by a major coordinated attack on Dyn, a leading domain name system (DNS) provider, that employed hacked connected devices including cameras, printers, routers, and other consumer-grade home devices. The hackers used these compromised devices to launch a distributed denial of service (DDoS) attack on Dyn, causing major disruptions to internet service worldwide. The devices were compromised due to lax security measures including unsecured routers and weak passwords that in some instances were unchanged from the default, which allowed the hackers to gain control of the devices and add them to a Mirai botnet. The hackers were then able to command the tens of thousands of devices to make thousands of server requests to Dyn each second, thereby overwhelming the system and bringing the DNS provider to its knees.

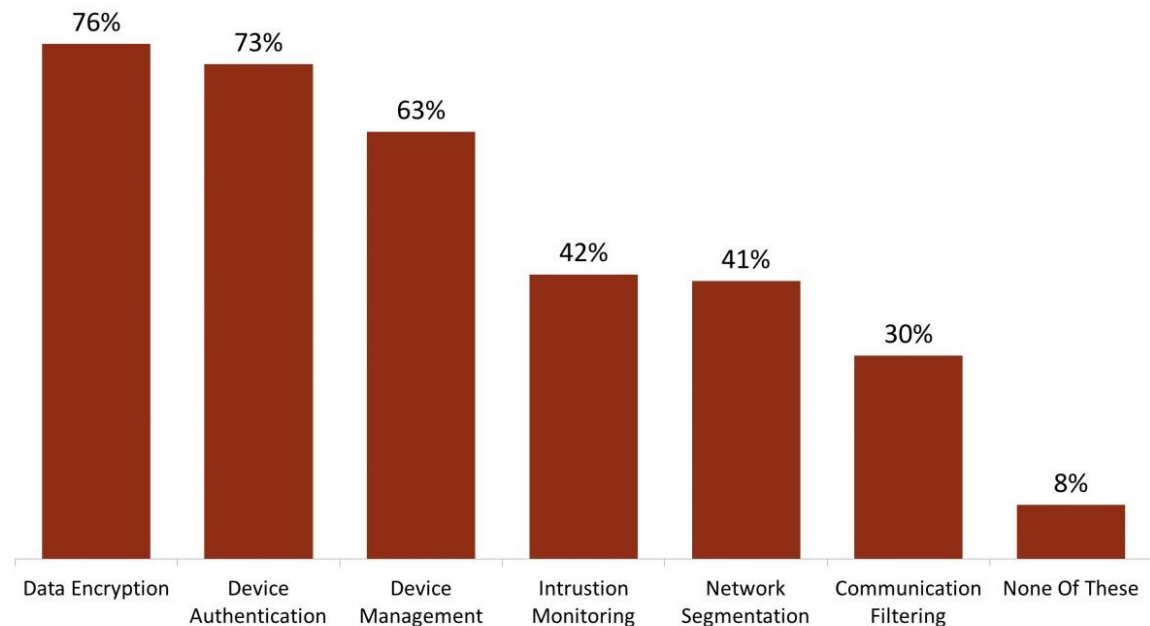
Consumer IoT products are uniquely vulnerable to these sorts of attacks. That's because they're often produced by companies that haven't developed connected products in the past, and therefore boast little experience to draw upon. In addition, consumers generally don't want to deal with security issues on their own — particularly if it means putting up with a cumbersome setup or diminished user experience. Device makers must strike a balance between developing secure devices that can resist hacks and presenting consumers with an easy setup process and seamless integration. A device that's extremely secure may be too complex to gain significant market share because it requires frequent password changes or too much user interaction, while a device that's not secure enough is vulnerable to hacks and could force the device maker to initiate a costly [recall](#) and possibly lose consumer trust.

Another complicating factor is that IoT devices are built around different computing hardware than traditional computers, and thus use less processing power and offer limited background processes. Traditional computers employ antivirus programs for security and require explicit user permission to greenlight processes, but IoT devices can't run these types of applications. **IoT security measures are most effective when built directly into the hardware, making use of specialized low-power [chips](#) that can implement end-to-end security, rather than relying on software-based security measures.**

Industrial and enterprise IoT solutions also come with a number of security concerns, but providers are more equipped to deal with such problems. They're built from the bottom up with security in mind, because buyers demand robust protection for their systems. BI Intelligence's survey found that 43% of executives at companies that have deployed or are looking into IoT solutions indicated security concerns were a major hurdle to implementation. However, these concerns are generally overcome in the enterprise space, as indicated by the choice of these companies to move forward.

Security Measures Providers Use In IoT Services

Global, 2016



Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=120 IoT Providers)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

Our survey data indicates that IoT solution providers and device makers offer a robust range security measures. Of those surveyed, 76% indicated that their products or services offer data encryption, 73% data authentication, and 63% device management. Only 8% of respondents don't utilize any of the common security measures they were asked about.

What to watch for in 2017: Sporadic breaches of consumer devices are likely to continue as current connected devices, especially for the smart home, sell at steady rates without increased security protocols. At the same time, new consumer devices will likely be deployed with better security measures in an effort to differentiate them from what's already available in the market. In the enterprise and industrial spaces, look for more solutions to implement security at the hardware level and for those protocols to integrate more closely with cloud-based storage platforms.

IoT MARKET OUTLOOK

The current growth in the IoT is a product of several years worth of preparation and drummed up interest. To better understand how we got to this point, we asked executives at companies that both have and have not yet implemented IoT solutions when they first looked into the IoT.

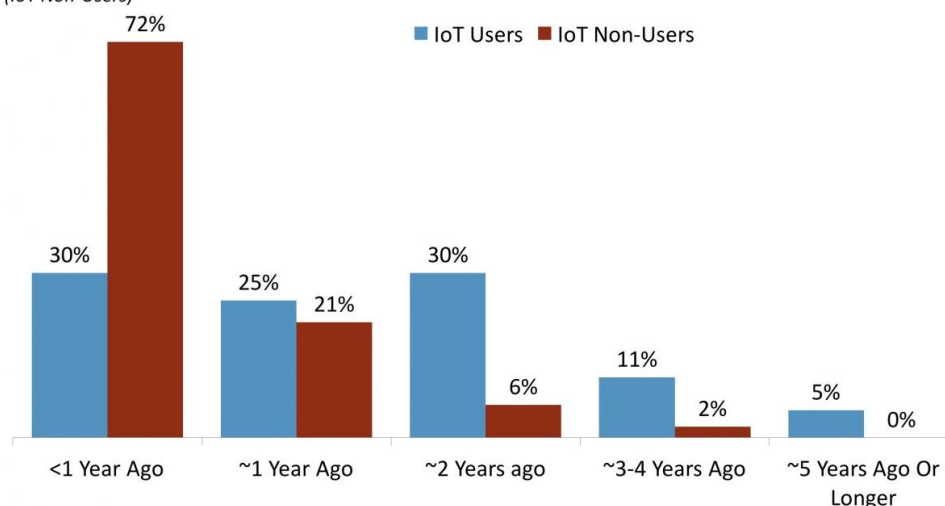
- **At companies that have implemented IoT solutions, 85% first looked into those solutions in the last two years.** The IoT has grown in prominence and practicality since 2014, prompting more and more companies to explore solutions to increase their efficiency and productivity.
- **Of those that have considered but not pursued an IoT solution, 72% indicate that their company discussed potential IoT programs within the last year, and 21% said such discussion took place about a year ago.** This can indicate one of two things: Either companies are just beginning to look into IoT solutions, or they have been forced to return to consideration of such solutions recently, and possibly repeatedly, and have not yet decided to make such an investment.
- **Given the sharp increase in consideration of IoT solutions, the number of devices used should continue to rise,** as more companies pursue IoT implementations to grow their businesses and remain competitive in an increasingly connected world.

The Timeline Of IoT Investigation

Global, 2016

Q: When did your company first start looking into IoT solutions? (IoT Users)

Q: When was an IoT solution last discussed or seriously considered within your company? (IoT Non-Users)



Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=218 IoT Users, 53 IoT Non-Users)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

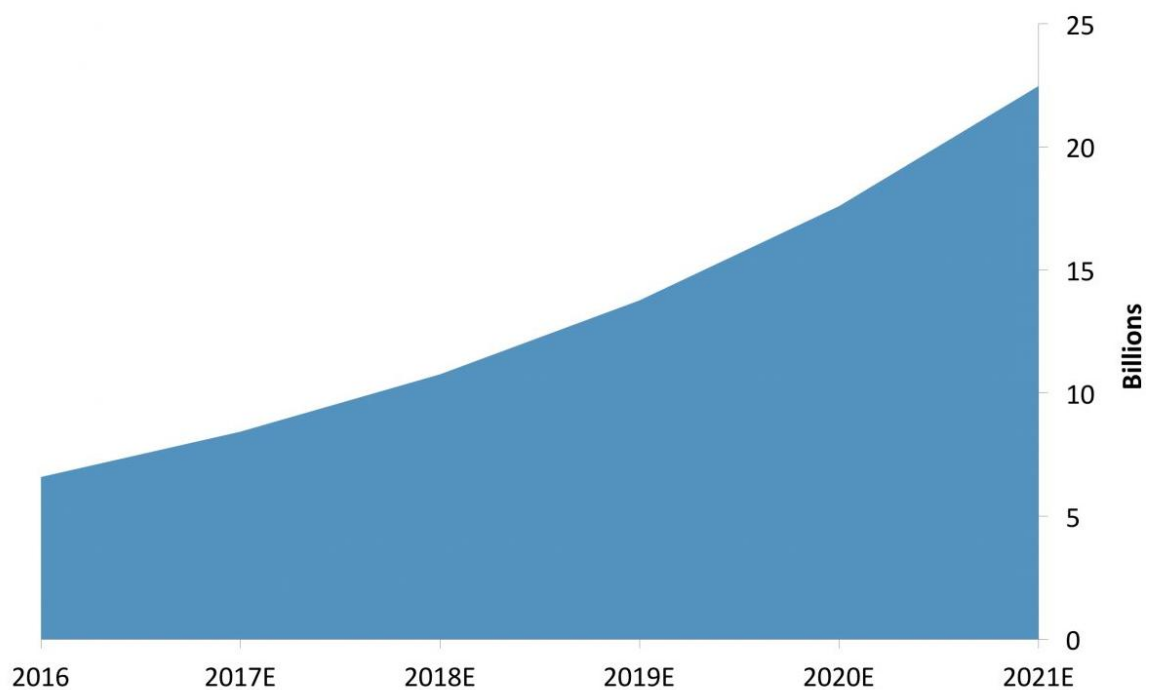
Recent advancements in the IoT ecosystem have set the scene for major growth in the IoT in the years ahead. In the next five years, marked increases in the number of IoT devices in use and strong growth in investment in IoT solutions are likely. This growth will lead to major increases in efficiency and productivity, as companies and platforms discover innovative new ways to deploy IoT devices and analyze the data they produce.

Device Installation

The IoT is poised to continue strong growth in the overall device install base over the next five years. This growth will be fueled primarily by commercial and industrial implementations, enabled by the burgeoning ecosystem, robust platforms, expanding networks, and tumbling hardware costs.

FORECAST: IoT Device Installation Base

Global, 2016-2021



Source: BI Intelligence Estimates and Business Insider Global IoT Executive Survey, 2016

BI INTELLIGENCE

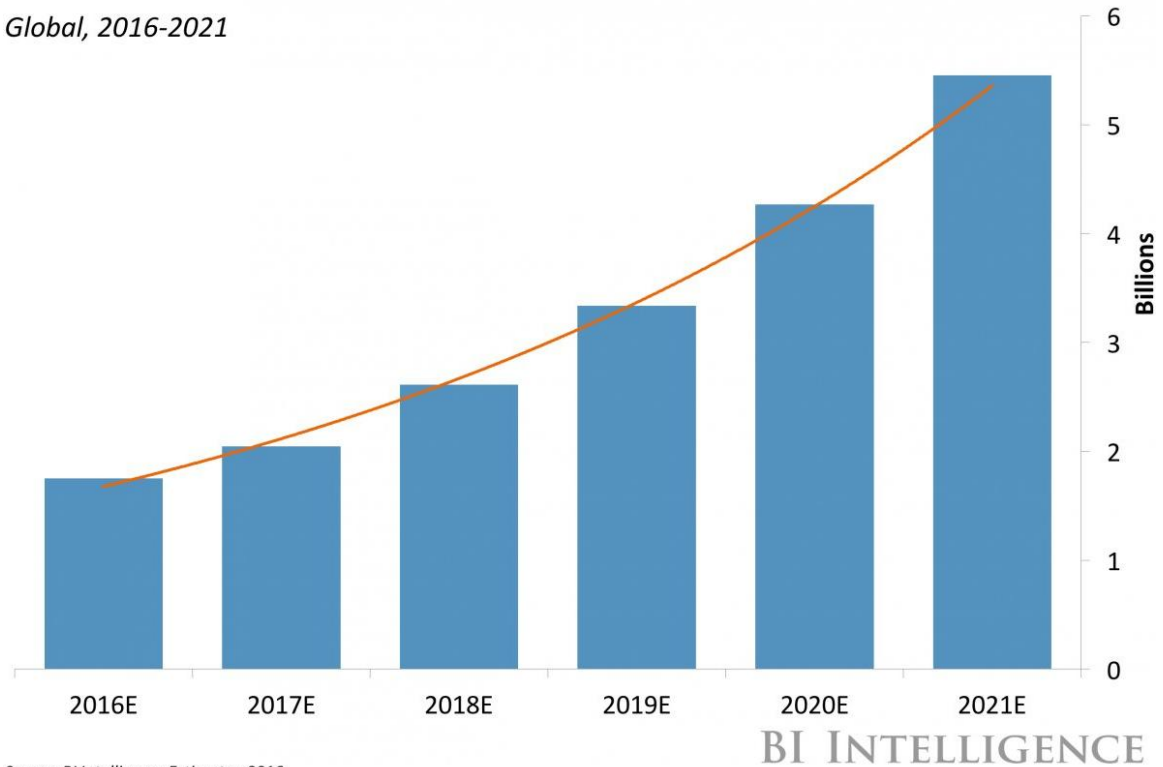
BI Intelligence expects that there will be 22.5 billion IoT devices installed worldwide in 2021. This estimate is based on analysis of various environments that could or already have deployed IoT devices, findings from our exclusive BI Intelligence survey data, and conversations with IoT decision makers.

Last year, BI Intelligence projected that there would be 24 billion IoT devices installed by 2020. That estimate has been lowered to account for a number of key trends in the IoT market:

- **Device consolidation:** Companies are using fewer devices to do more. Devices are strategically placed throughout operations to gather the maximum amount of data with the smallest necessary investment and minimal physical and digital footprint.
- **Increasingly complex and powerful analytics:** The power and capabilities of analytics have grown greatly over the past year as IoT platforms have incorporated more advanced machine learning techniques that enable them to extract more value from data over a shorter period of time.
- **Network stagnation:** The low adoption rates of IoT-specific networks and continued reliance on Wi-Fi and cellular networks for transmission have limited the number of devices that can be put into the field. Devices that use lower-power networks are able to be placed more remotely and require smaller and cheaper batteries.

FORECAST: IoT Device Installations

Global, 2016-2021



Source: BI Intelligence Estimates, 2016

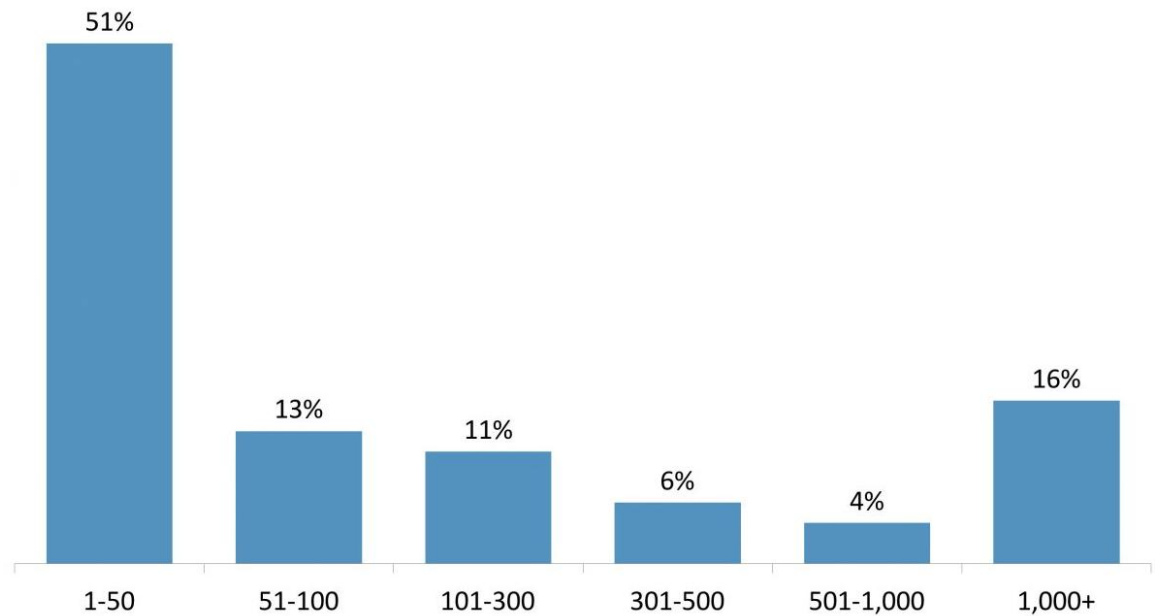
Meanwhile, the number of IoT devices shipped through 2021 will be well into the billions annually. The number of devices installed each year will track with the overall installation base but slightly outpace it, as a small portion of installed hardware will require replacement, either due to failure or upgrades for shorter-lifecycle devices. Beyond the timeline of our forecast, the number of devices shipped will likely continue to rise at increased growth rates due to greater affordability and the adoption of LPWANs.

IoT Implementations

BI Intelligence's survey highlighted several trends regarding IoT solution implementations, which we define as device installations at a particular organization as part of a concerted and directed plan. A single implementation can involve installing multiple IoT devices, with the number depending on the needs of that company or group.

The Number Of Devices Companies Use In Their IoT Solutions

Global, 2016



Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=235 IoT Users)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

Companies implementing the IoT are focusing on smaller device installations:

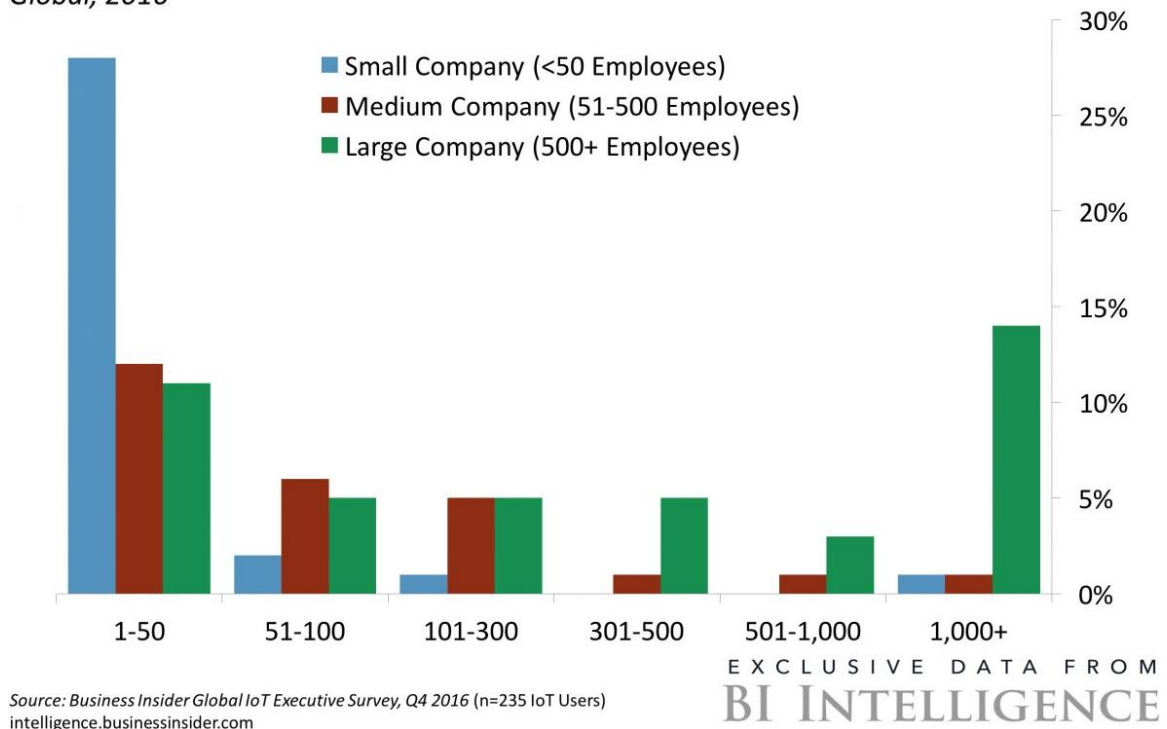
- According to exclusive BI Intelligence survey data, at companies that have or are in the process of implementing IoT solutions, **51% of respondents say their companies will use fewer than 50 IoT devices**. A further 13% say they are using or will use 51 to 100 devices, and 11% indicate between 101 and 300.
- **Only 16% indicated that their companies are using or will use more than 1,000 IoT devices**. Deploying IoT devices in large numbers requires major capital investments, which companies are likely reluctant to pursue until they fully understand the technologies involved.

One key factor that drives the size of an IoT deployment is company size. While the majority of IoT projects employ less than 50 devices, most respondents with this size IoT project were at companies with fewer than 50 employees.

- **Smaller companies are pursuing primarily smaller IoT projects**, commensurate with their available resources and the scope of their overall operations.
- **More substantial IoT projects seem concentrated predominantly at companies with more than 50 employees**. These companies are able to leverage their resources to finance larger IoT projects.
- **The largest IoT implementations, with over 1,000 devices, were generally found at large companies with over 500 employees**. Only companies with the greatest needs and resources to make major strategic investments are able to finance large IoT projects.

Company Size And The Number Of Devices Used In IoT Solutions

Global, 2016



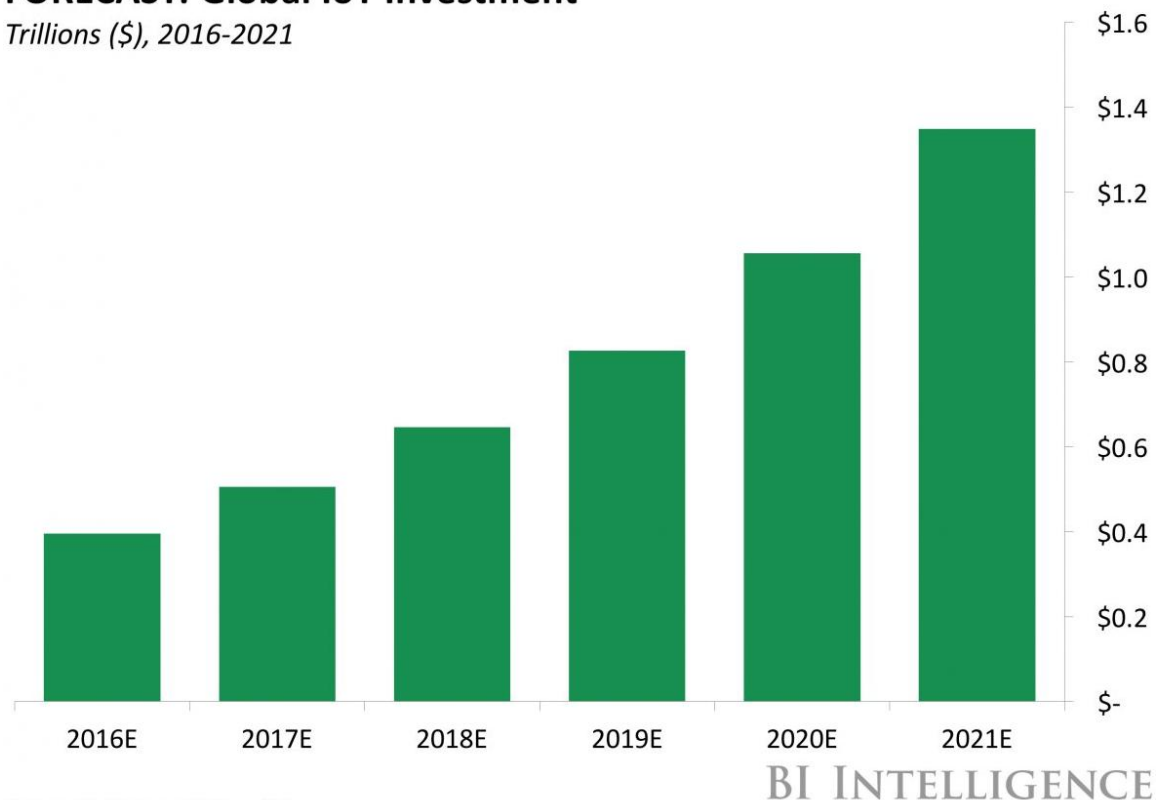
Large IoT implementations are likely to remain generally limited to larger companies with needs that justify them. Although some smaller organizations with specific operational needs may also venture into larger projects, they're likely to move forward only after smaller experimental pilot programs. In addition, we anticipate that many companies will look to minimize the number of devices that they require for an implementation, relying more extensively on multipurpose sensors such as cameras that, when linked to cloud-based software, can take the place of multiple single-use devices.

Investment

As the number of IoT devices installed and in use increases, so too will the amount of capital invested in the IoT. Companies, consumers, and governments will spend trillions of dollars to grow this ecosystem.

FORECAST: Global IoT Investment

Trillions (\$), 2016-2021

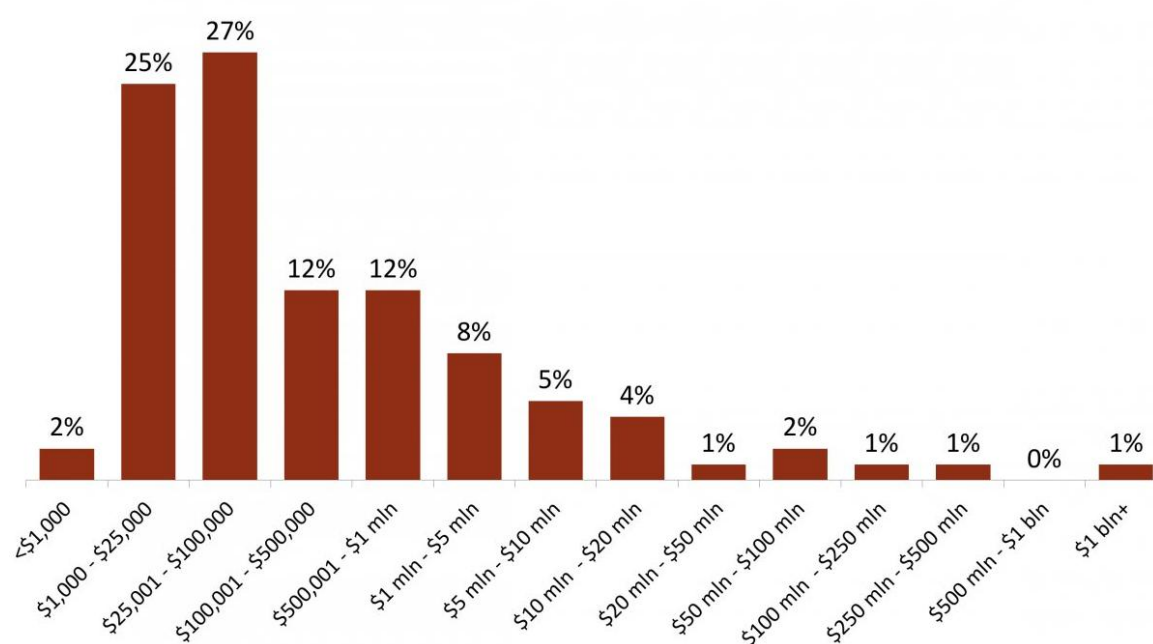


BI Intelligence estimates that annual spending on the IoT will rise from just under \$400 billion in 2016 to \$1.35 trillion in 2021. This forecast is based on device projections, platform cost and growth projections, and data on device operation and associated costs. **In total, we expect \$4.8 trillion in IoT spending over the next five years.**

For a more detailed picture of investment in the market, BI Intelligence's survey asked executives at companies that have or are in the process of implementing IoT solutions what levels of investment they've made or plan to make in such technology.

Companies' Total Planned Investment In IoT Solutions

Global, 2016



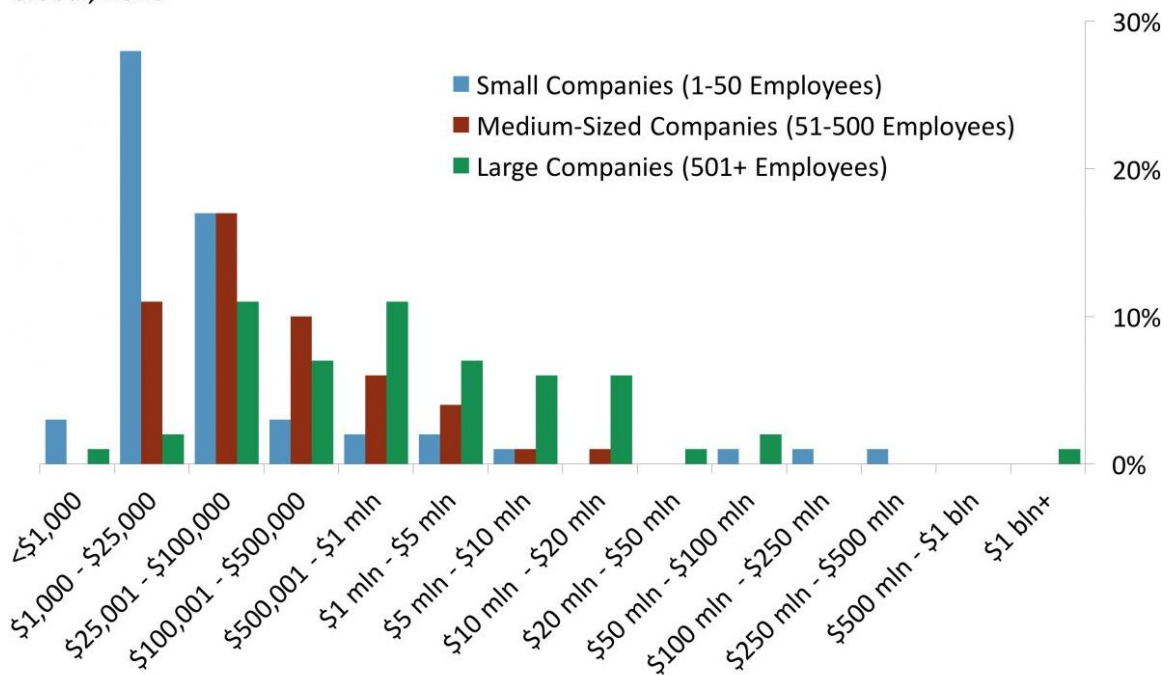
Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=164 IoT Users)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

The majority of companies surveyed plan to invest less than \$100,000 in IoT implementations, with 25% of respondents investing between \$1,000 and \$25,000, and 27% spending between \$25,001 and \$100,000. There are fewer responses as the investment numbers grow larger, though the paucity of companies able to make multimillion dollar investments in the IoT provides some explanation for this trend. It's important to bear in mind, though, that a single investment in the \$10 million to \$20 million range represents the same overall investment in the IoT ecosystem as 10 investments in the \$1 million to \$2 million range.

Total Planned IoT Investment By Company Size

Global, 2016



Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=164 IoT Users)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

Much as with the number of devices employed in IoT solutions, company size is related to the magnitude of an IoT investment.

- Smaller companies generally concentrate on smaller IoT investments, with 76% of companies with fewer than 50 employees investing between \$1,000 and \$100,000.** Only a handful of respondents at these smaller companies reported that they made significantly larger IoT investments, highlighting the resource limitations of such firms.
- Mid-size and larger companies dominate the realm of larger IoT investments.** Respondents at companies with more than 500 employees make up the largest share by far of those with an IoT investment of \$500,000 or more under their belt. Companies with the resources to employ a substantial number of workers also often have the resources to allocate funding for large, potentially transformative IoT projects.

Ongoing investment in the IoT will drive growth and enable the proliferation of devices around the globe in the years ahead. The trillions of dollars expected to pour into the IoT through 2021 will radically alter numerous fields and change companies' practices across industries.

THE TOP THREE TRENDS IN THE IoT

Based on our own research, analysis, and forecasting of the IoT market, as well as conversations with industry executives, we've identified three key trends likely to shape the IoT in 2017:

1. Companies are focusing on the IoT as part of an overall digital transformation.

Businesses are making investments to transform their operations and make them agile enough to compete in the increasingly digitally engaged marketplace. The IoT is a central part of this transformation.

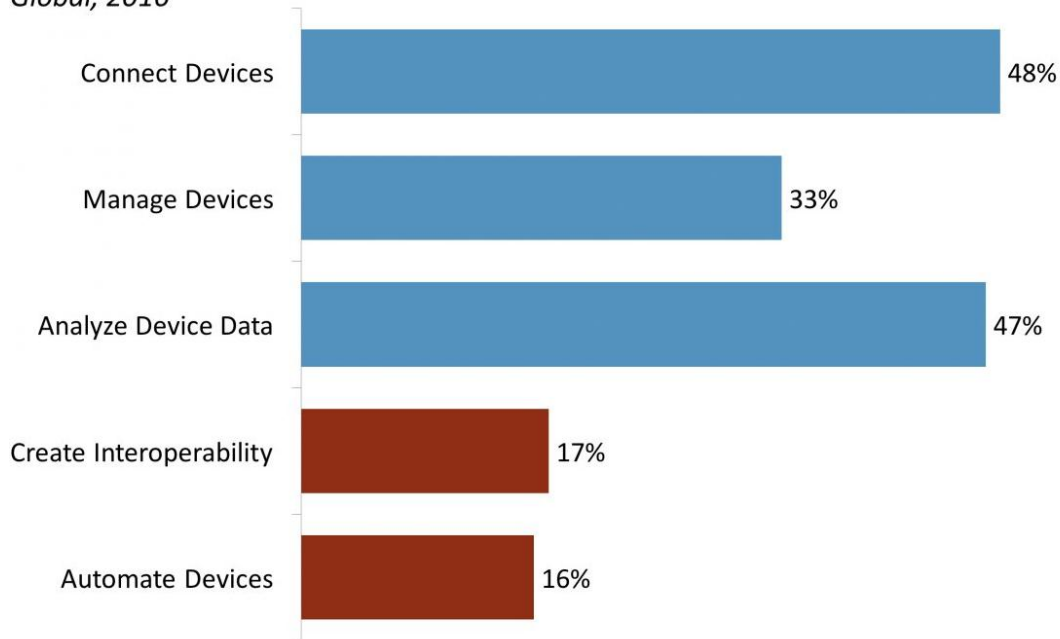
2. The IoT is becoming overcrowded, and the market will see massive consolidation in the years ahead. There are a vast number of IoT companies; some have only a handful of employees, while others employ thousands of workers around the globe. A key trend within the IoT recently has been the consolidation of these providers through numerous mergers and acquisitions. Small providers have been purchased by larger ones, mid-size providers have been bought by even bigger companies, and some major players have been purchased by giant corporations.

In the past year, IoT platform Jasper was [acquired](#) by Cisco, fleet-management service provider [Fleetmatics](#) by Verizon, and microchip design firm [ARM](#) by Softbank. Meanwhile, exclusive data from our BI Intelligence survey indicates that 58% of IoT solution providers or device makers have seen at least some consolidation within the market for their products or services. In the years ahead, the companies that are acquired will likely be those with a niche product or service that larger companies want to help build out their own IoT offerings.

3. The IoT is still not meeting its full, five-stage potential. IoT deployments can be seen as having five separate and distinct stages: connecting devices, managing devices, analyzing device data, creating interoperability between devices, and automating devices.

The 5 Stages Of The IoT — What Companies Do With Their IoT Solutions

Global, 2016



Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=233 IoT Users)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

Each of these stages brings new and increased value to an IoT solution, allowing a user or organization to gain greater insight and efficiency. Moving along the track from the first stage to the fifth incrementally yields these gains.

- **Connecting devices:** This is the stage in which internet connectivity hardware is embedded into “things.” Once a device is connected, an end user can start to manage it and collect data about its use. According to our survey, **48% of respondents indicated that their companies are connecting devices with IoT solutions.** By connecting devices, users gain visibility into where devices are and what they are doing. For example, a logistics provider can add GPS trackers to trucks to track where drivers are in their routes.

- **Managing devices:** The second stage is reached when users start to manage the devices in an IoT deployment and the data the devices produce. They can monitor devices, implement authentication and security practices, and control data collection. Only 33% of respondents in our survey stated that their companies use IoT solutions to manage their devices, but this is likely because it is common to conflate connecting and managing devices. By implementing the first two stages, companies can start to see value from their IoT solutions. That logistics provider could implement security controls, requiring drivers to login through a secure system that protects and monitors the vehicles.
- **Analyzing data:** The third stage is to analyze the data generated by IoT devices and create actionable insights. This can power benefits of the IoT like predictive maintenance. However, **less than half of companies that have implemented an IoT solution (47%) analyze the data their devices generate**, according to our exclusive survey data. This is likely because it can be difficult to get actionable insights from the massive volumes of data produced. Companies like Microsoft and Cisco are developing platforms to help with these analytics issues, but since no two solutions are alike, each model has to be adjusted to fit the specific devices within each IoT deployment. If our hypothetical logistics provider were to implement the third stage of the IoT, it would be able to take the data gathered from tracking vehicles and use it to optimize driver routes.
- **Interoperability:** The fourth stage is to make the devices within an IoT deployment talk to each other. For example, in a smart home, connected lightbulbs may speak to the connected door locks. If the lights are turned on, they will tell the door locks that someone is home. Reaching this stage requires meeting all of the steps above and equipping devices with extra software that enables them to coordinate with one another, which is extremely difficult — **only 17% of companies that have implemented IoT solutions utilize devices that talk to each other**, according to our survey data. Interoperability will be easier to achieve over time once standards are put in place that create a common language for devices to use, leading to immense increases in efficiency. For example, if the logistics provider were to put its truck-based systems in communication with its warehouse systems, restocking orders could be triggered when an item moves from the warehouse shelf to a delivery vehicle.

- **Automation:** The fifth and final stage is to automate portions of the environment where the IoT solution operates. For instance, if the connected light bulb senses someone is home and their behavior patterns indicate they are sleeping, the light could signal the door locks to lock and other lights to turn off. This requires machine learning and advanced AI to achieve, and it's often associated with replacing workers with machines. **Less than 16% of respondents at companies surveyed by BI Intelligence that have implemented IoT solutions use their IoT devices to automate portions of the workflow.** The logistics provider could, by implementing automation, use a fully robotic warehouse that immediately responds to requisitions by moving goods onto an autonomous delivery vehicle. This type of system would enable the company to create the maximum savings and greatly increase operational efficiency.

As the technology within the IoT continues to advance, we expect to see more companies move toward interoperability, and eventually automation. Right now, the greatest barrier to automation is that the technology behind the IoT is not mature enough to support it. For example, a broad analytics suite can be applied in multiple settings and serve many customers, but it isn't able to process data in a precise enough manner to enable automation. To fully automate workflow, IoT providers will need to better specialize their product offerings to meet each company's specifications.

Achieving the later stages offers great financial benefits and savings, but also comes with a number of costs. While advanced systems would in most instances substantially reduce the size of a company's workforce, they will also require sizable capital investments. In addition, moving into partial or total automation can substantially alter a business' culture. A careful consideration of the costs and benefits is necessary before a company takes on a shift toward complete automation.

SOLUTION PROVIDERS BEHIND THE IoT

IoT providers create, implement, and maintain IoT solutions. They bring to the table some combination of specialized hardware and/or software, as well as an understanding of the connected technology that characterizes the IoT.

The most successful and effective providers, however, also bring contextual knowledge of a particular field or industry. Throughout the enterprise and industrial IoT, providers are best able to assist their clients by gaining (through experience and smart hiring) insights into client operations, rather than just leveraging knowledge of IoT solutions. In addition to this technical assistance, though, the provider can offer guidance on how to update hiring needs or what sorts of retraining will be useful in light of these transformations. The provider can also work with the client to transform maintenance and upkeep policies from reactive to proactive and preventive, maximizing the utility of the IoT investment.

Even though IoT providers are starting to build full-stack solutions, most of the offerings available right now serve only certain functions. As a result, some IoT end users will make use of multiple providers in putting together a complete IoT setup within their company. The providers that tout the best value are ones that tailor solutions to each client. The IoT requires communication and translation, and every IoT solution differs slightly, forcing changes to practices on both sides to find optimal efficiency.

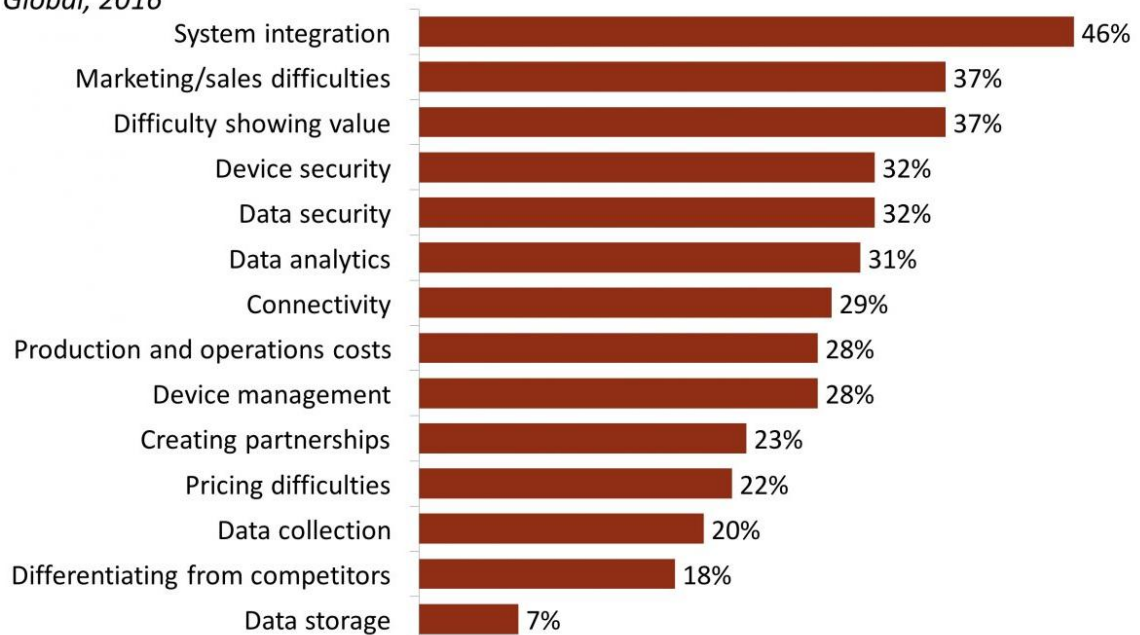
Challenges For Providers

IoT providers must develop services and products that appeal to potential users, assuage their concerns, and provide them with value to justify potentially substantial investments. To provide more color on the obstacles they face, we asked executives at IoT providers about the primary challenges that they have faced in developing IoT services.

- System Integration:** Forty-six percent of respondents identified system integration as a main challenge in developing an IoT service, according to BI Intelligence's survey results. Executives who are responsible for spending and technology policies will not necessarily be versed in the details, benefits, and challenges of engaging with the IoT. Their primary concern is with operations and profits, and they do not want to risk disruption for the sake of technological innovation on its own. As a result, companies are likely looking for IoT solutions that can seamlessly slot into existing operations. However, these often involve numerous disparate systems and solutions within a single company, and the different configurations and combinations across companies within a single industry can create major difficulties for IoT providers.

Challenges Providers Face In Developing An IoT Service

Global, 2016



Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=120 IoT Providers)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

- **Reaching customers:** Thirty-seven percent of respondents said they face marketing and sales difficulties, and the same percentage have difficulty showing value. Such difficulties demonstrate the educational hurdle that IoT providers must overcome to develop a successful service. The benefits and uses of the IoT can be difficult to explain, and this often requires a contemplative approach from providers to prove their worth. This will likely come into greater focus as these companies seek to pair technical knowledge with clear explanations and illustrative examples that demonstrate the benefits of implementing IoT solutions.
- **Data Analysis:** Another hurdle that IoT providers face is properly analyzing data, with 31% of respondents identifying it as a challenge. This is evident in other studies, as well. According to a survey from Honeywell and KRC, 39% of industrial companies are not using big data and engaging with the IoT because they do not have the proper personnel to create and analyze the data. Data analysis practices and communication are key responsibilities of IoT providers, and ones that they must bolster to expand their user bases.

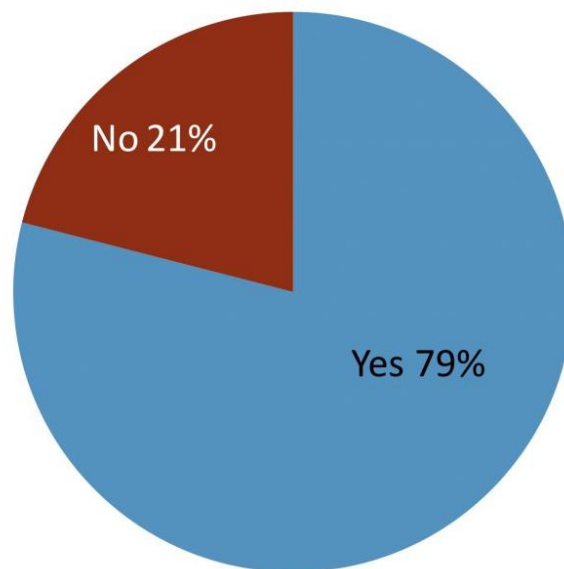
Overall, the most substantial challenges to IoT providers are based on communication with potential clients and with the systems that those clients already employ. IoT providers are aware of these challenges, however, and are taking steps to refine communication strategies and better explain the value in implementing IoT solutions to potential clients. In addition, we expect system integration issues to fade in prominence as IoT providers mature and gain greater experience with the variety of systems commonly employed within the industries they serve.

Data Collected By Providers

The top selling point for the IoT is that businesses are able to benefit from the massive wealth of data that can be generated by connecting devices throughout their operations. But IoT providers are also able to collect data from the devices that they operate as part of their services to other companies, and do so on large scales.

Do IoT Providers Collect Data From Their Devices And Services?

Global, 2016



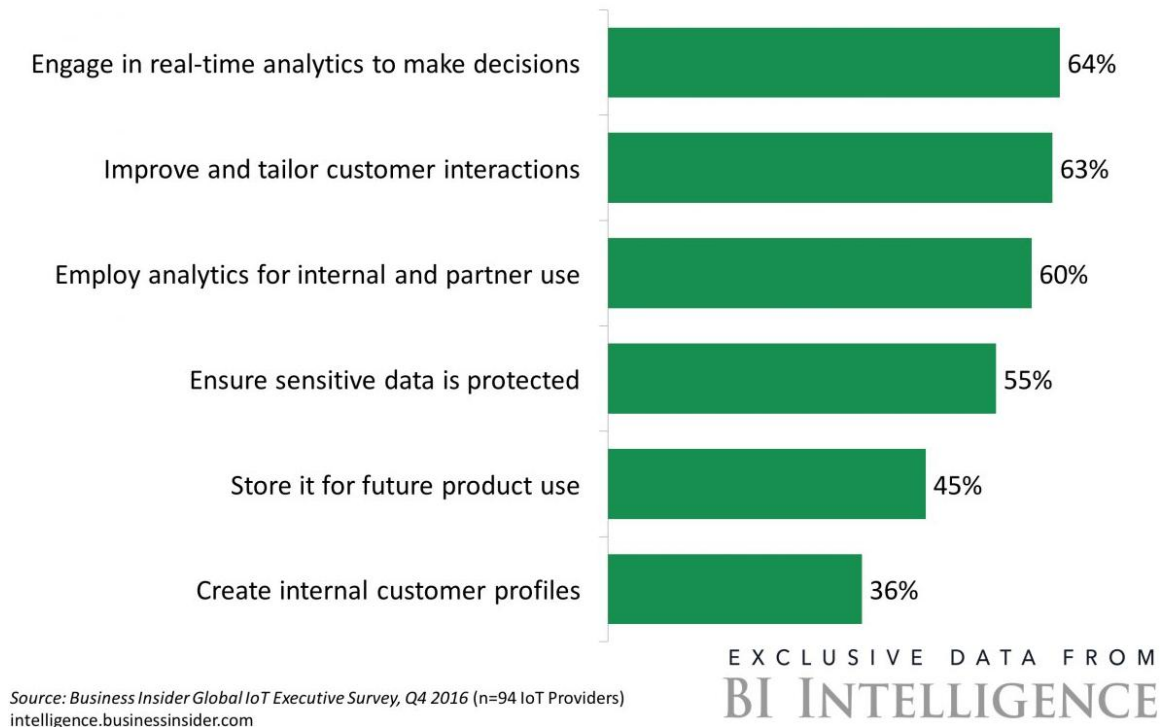
Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=120 IoT Providers)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

According to our recent survey, **79% of IoT providers collect data from the IoT devices they provide or service.**

How IoT Providers Use The Data They Collect

Global, 2016



The providers that collect data from their devices make use of the data in a variety of ways:

- **64% of respondents indicated that their companies use the data to engage in real-time analytics and make decisions.** Similarly, 60% of companies employ analytics for internal use, and 45% use it for future product use. The benefits that data from IoT solutions can provide are well known to providers of such services, as they sell their offerings to clients based on them. Therefore, it makes sense that IoT companies themselves would engage in data analytics to improve their own services and provide better IoT solutions for their clients.
- **63% of respondents said that their companies use data to improve customer interactions and tailor interactions with the clients from which it's collected.** For example, a provider may gather data on a client's equipment in order to provide advice on when it needs to be upgraded or replaced. It could then offer recommendations on options for new equipment based on the client's specific needs.

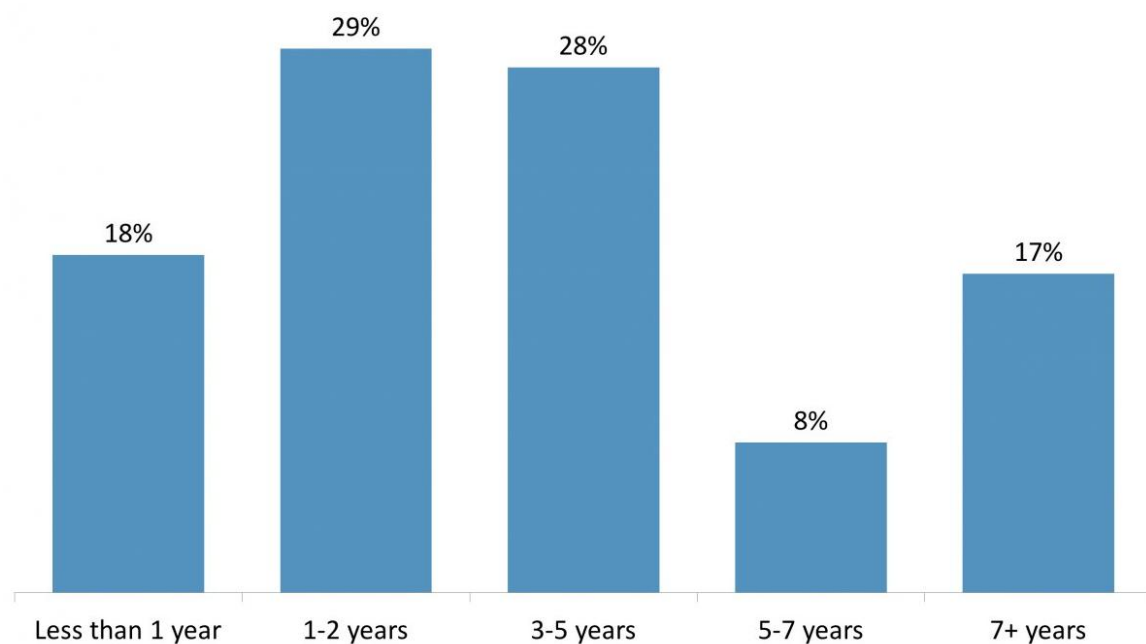
- **55% of providers store this data securely.** IoT solution providers often act as cloud providers or intermediaries for their users. This means they must hold and secure the data that they extract from connected devices for their own and their clients' usage. Storing data is key not only because the data is valuable in its own right, but also because it can be leveraged to provide new analytic insights later on. Data gains new and increased value over time, and companies and analysts can use it identify longer-term trends in the future. IoT providers are responsible for ensuring that the data remains available for such analysis.

The Age Factor

As discussed above, many IoT users only began looking into and implementing IoT solutions in the last two years. To put that finding into better context, we asked respondents about the length of time their companies have been engaged in the IoT.

Length Of Provider Activity In The IoT

Global, 2016



Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=120 IoT Providers)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

BI Intelligence data shows that IoT providers have generally been involved in the IoT for slightly longer than the companies they serve:

- Although the majority of IoT users first looked into IoT solutions within the past two years, **53% of IoT providers have been active in the IoT for three years or longer.** This makes sense, as to develop a competitive IoT service, providers must plan it out and develop protocols to address the concerns that will emerge from its use. Issues pop up that demand attention, and companies that plan to offer IoT solutions need time to make their offerings issue-free before wide release.
- Another explanation for the longer engagement of IoT providers is that many of these companies are involved in business activities other than IoT services. As a result, **these companies are able to sustain an IoT service while it's in a developmental phase without requiring outside investment.** Operating under a larger business with multiple revenue streams enables IoT providers to take their time, affording them the ability to develop and launch complete products.

THE IoT END USERS

There are three broad groups of IoT end users: consumers, governments, and enterprises. Each uses IoT solutions in varying ways and offers different returns for IoT providers.

- **Enterprise is the most targeted group by IoT solution providers.** The enterprise space is the largest potential market for providers, and should continue to see rapid adoption of IoT solutions in the years ahead.
- **Governmental organizations, including cities, education, and defense, are less targeted, but still have promise.** Projects won by solution providers in these areas are less frequent but can be large in scale.
- **Consumer devices, including smart home devices and wearables, are less targeted and don't offer the same growth potential as enterprise or government customers.** However, the consumer IoT market has long-term growth potential.

Consumer

The consumer IoT makes up the portions of the IoT that serve end users their home or personal life. The most common types of consumer IoT devices include smart-home devices, such as the Nest Thermostat or the August Doorlock. In addition, fitness trackers and wearables that don't run apps are considered consumer IoT devices. Connected cars also fall into this category, though automakers see tremendous benefits from connecting their cars to the internet, as well. Overall, the consumer IoT market is small in comparison to the overall IoT market and experiencing relatively slow growth.

The smart-home market, in particular, is still in the very early stages of growth.

Approximately 30% of US consumers own a single smart-home device, which shows relatively low growth from 2015, according to a Sylvania survey. The market is plagued by high prices, difficult installation, and long replacement cycles. It is in desperate need of a killer product to push the market forward, much like how the iPhone propelled the smartphone market.

Speaker enabled voice assistants, like the Amazon Echo and the Google Home, may be the transformative breakthrough that the smart home market needs, but voice assistant speakers are still in the very early stages of adoption. Overall, we expect slow growth in the smart home market over the next five years — the market will undoubtedly take off eventually, but it likely won't see the explosive growth that the smartphone market witnessed anytime soon. In 2017, we expect more retailers to begin to offer smart-home installation services in conjunction with smart-home devices. This will help alleviate the difficulty consumers have with installation.

Fitness trackers and wearable devices, meanwhile, have grown in popularity over the past year, especially in emerging markets, such as [India](#).

This is primarily because fitness tracker makers have been able to lower prices and make them affordable to the mass market. Right now, much of the growth in the fitness tracker and wearables market comes from healthcare segments in developed and developing markets. For example, some insurers and employers offer rewards to fitness tracker users who exercise frequently, as it reduces their chance of chronic health issues. However, it's likely smartwatches will eventually displace fitness trackers as prices fall and functionality increases. In 2017, more companies will seek to use wearable technology to track worker movements. For example, workers' movement on a factory floor can be monitored and tracked to optimize product routing and efficiency.

Connected cars make up one of the fastest growing segments of the IoT, primarily because automakers are rapidly connecting the cars they produce in order to collect data about vehicle use. This can improve future cars and enable automakers to send over-the-air updates to prevent recalls. In addition, an increasing number of consumers are demanding added connectivity to their vehicles so that they can access the web in their car. Overall, connected-car shipments [are set to grow](#) from 21 million in 2016 to 94 million in 2021, representing a 35% five-year compound annual growth rate (CAGR). In 2016, an increasing number of automakers began to integrate Apple's CarPlay and Android Auto into their car's infotainment center. This trend is poised to continue in 2017 as more consumers look for their infotainment center operating system to work with their smartphone's OS.

Government

Increasing urbanization is driving cities to adopt digital technologies to improve efficiency. These projects can include smart energy management systems, public safety initiatives, public transportation, and more. Such implementations often involve large scale projects that require significant investments, but they can also have significant returns. For example, Barcelona invested €82 million (about \$86 million) in its smart city initiatives and saw a GDP impact of €85 million in one year.

Contracts for smart-city initiatives can be fruitful for an IoT provider. However, winning a municipality's business depends on appropriately positioning the solution being offered. For example, an IoT provider may play up its solution's public safety benefits in one country, while emphasizing its sustainability features in another. This is common within the IoT space and speaks to current adoption trends in different regions of the world.

- **Europe:** The European Union (EU) has been pushing its member countries to implement smart-city initiatives, and as highlighted in BI Intelligence's [Smart Cities report](#), the region is generally at the forefront of adoption. The driving factor for European countries is to meet sustainability goals and reduce fossil fuel consumption. They intend to reduce total greenhouse gas emissions to 20% below than 1990 levels, while also increasing energy efficiency by 20%. This will require significant overhauls of countries' power infrastructures. As a result, IoT companies targeting Europe may do well by positioning their product as energy-first.
- **Central and South America:** Outdated infrastructure, coupled with rapidly increasing urbanization, is prompting cities in Central and South America to revamp infrastructures to help manage congestion. In particular, smart transportation initiatives are being put in place to help reduce traffic congestion. For example, Santiago, Chile, has implemented a network of sensors to track motor vehicle traffic. Further, the city implemented a toll system that charges more at peak times. However, most of these projects are taken on at the municipal level, with very little support from central governments in the region.

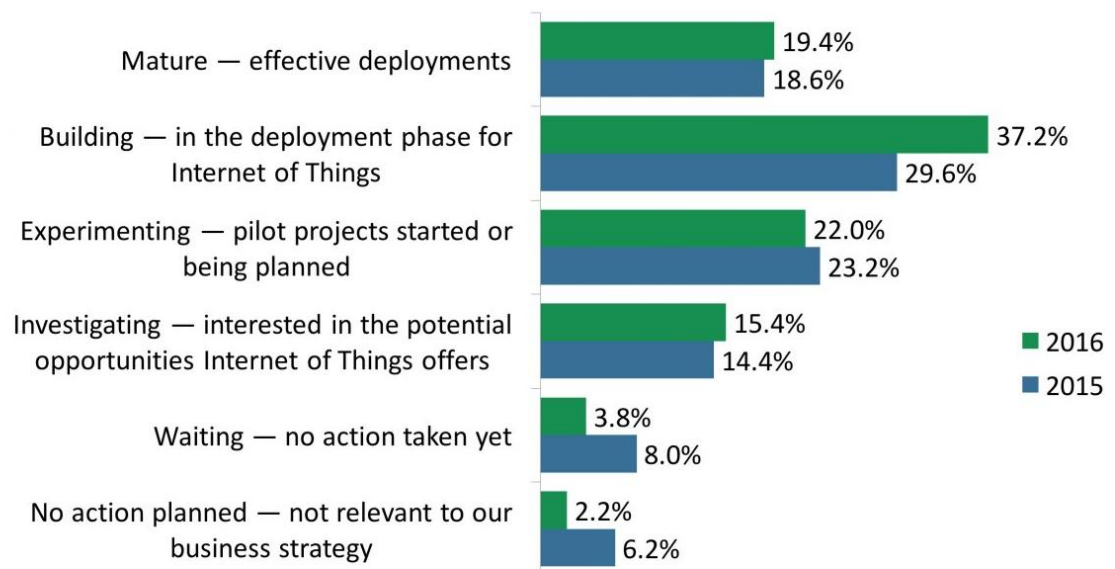
- **Asia:** Asia boasts many countries that are supporting smart city development. For example, China's Ministry of Housing and Urban and Rural Development has set aside \$16 billion for smart city projects, while India has allocated \$15 billion, and Singapore has allocated \$13 billion. Many developing Asian cities are implementing these technologies from scratch, as opposed to revamping infrastructure. In more developed cities, they are investing to catch up to European cities in efficiency and prestige.
- **North America:** North America is the most densely urbanized region, [according](#) to the UN, but it's lagging behind in smart-city development. This is primarily due to a lack of budget for such initiatives. However, the top use case for smart city projects in North America is public safety, with a number of programs aimed at reducing crime. For example, New York and Camden, New Jersey, have [tested](#) gunshot-detection systems, enabling law enforcement to respond faster.
- **Africa:** Africa is expected to see an increase in urbanization over the next few decades, which should accelerate smart city growth. The most pressing initiative is to expand public internet access throughout the region because it lacks legacy infrastructure. This would mirror programs in developed markets like LinkNYC. Once internet access becomes more widely available, it's expected that further smart city initiatives will follow.

Enterprise

Businesses are and will continue to be the top adopter of IoT solutions. This is primarily because they have the resources to invest in the IoT, and see significant benefits from doing so. As IoT providers develop more products and companies considering IoT solutions evaluate them, look for even greater adoption of the IoT within the enterprise sector.

US Mid-Market Companies' Stage Of IoT Development

Q: As growing numbers of devices are networked, internet-enabled, and take action without human intervention, which term most closely describes your organization's current use of the Internet of Things (IoT)?



BI INTELLIGENCE

Source: Deloitte, 2016

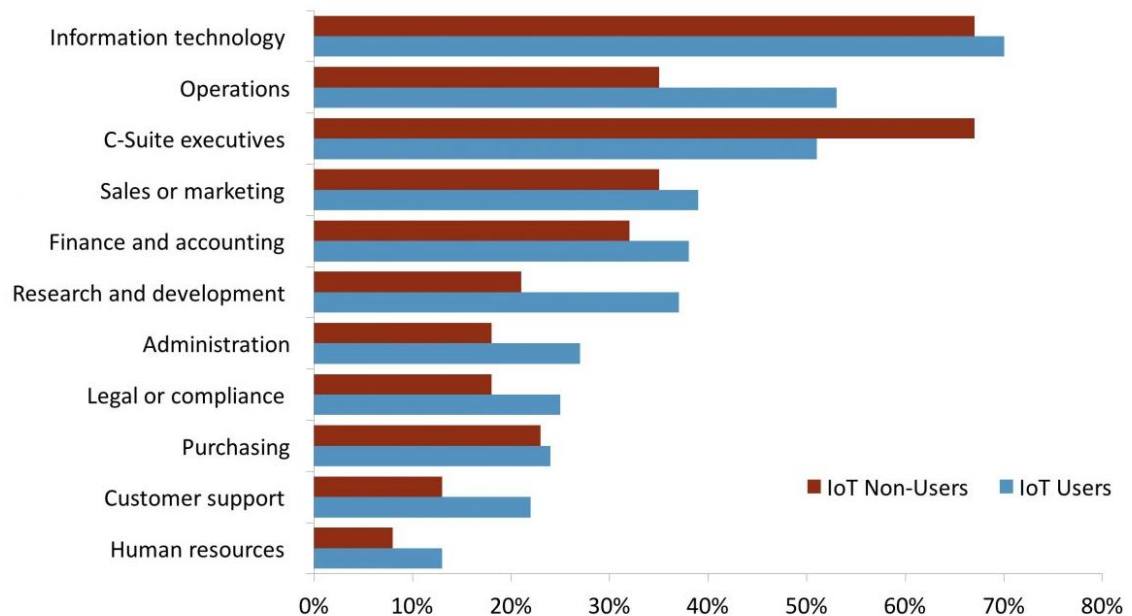
But the path from exploring the possibilities of the IoT to implementation is a long one. Indeed, the decision to implement IoT solutions generally occurs at the end of a lengthy process that includes several stakeholders. And those making such decisions need to account for the benefits of IoT adoption as well as the challenges a company may face in implementation.

Enterprise Decision Makers

As a company decides whether or not to tackle the IoT, who is brought into the decision-making process can have a meaningful impact on the decision that is made. To better understand this impact, BI Intelligence asked both those that had and hadn't implemented IoT solutions which groups were involved in the conversation.

Departments Involved With IoT Decision-Making Process

Global, 2016



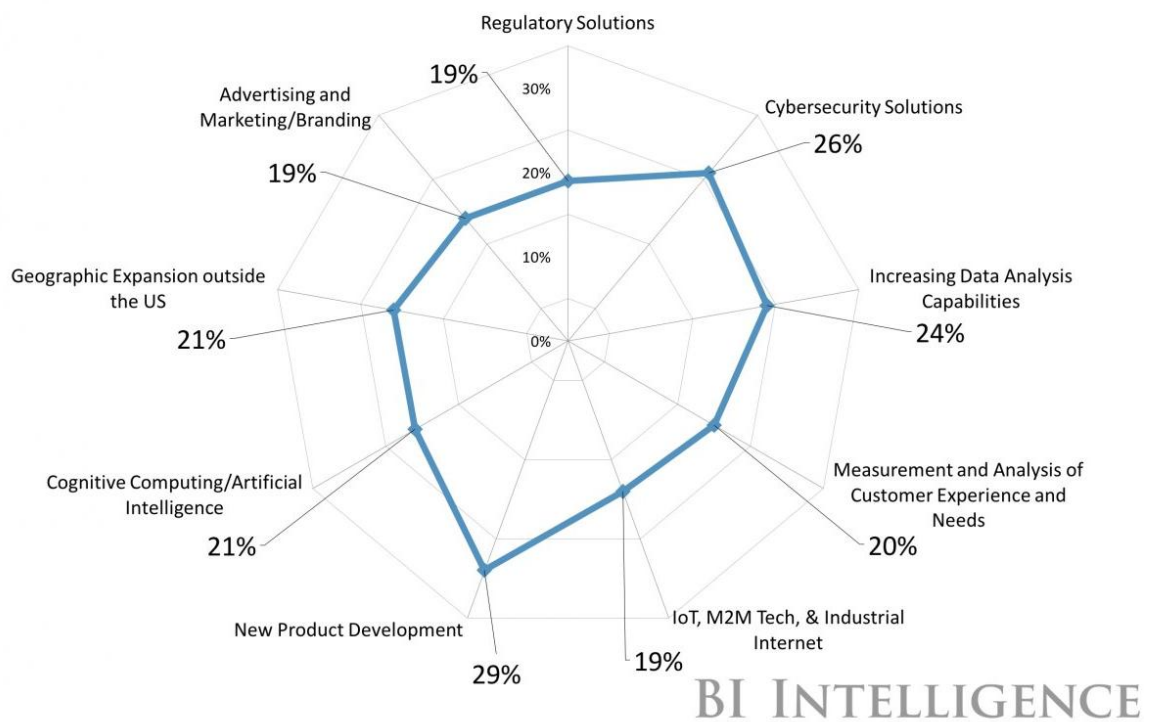
Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=232 IoT Users, 84 IoT Non-Users)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

- **Information technology (IT) was the most-cited department involved in the decision-making process**, according to our exclusive survey data. At those that had implemented an IoT solution, a slightly higher (70%) percentage of respondents indicated the IT department was involved, compared with those that decided against implementing an IoT solution (67%).

- **Operations was much more heavily involved in the decision-making process at companies that moved ahead with implementing an IoT solution.** This signals that companies that implemented an IoT solution were aiming to improve their day-to-day activities by involving operations teams in the decision-making process. Improving these functions offers an immediate return, which is a powerful enticement for implementation.
- **C-suite executives were more involved in the decision-making process at companies that chose not to implement an IoT solution.** This may show that those trying to provide IoT solutions to companies were unable to articulate the value of the solution to upper management.

CEO Investment Priorities In Building Agility

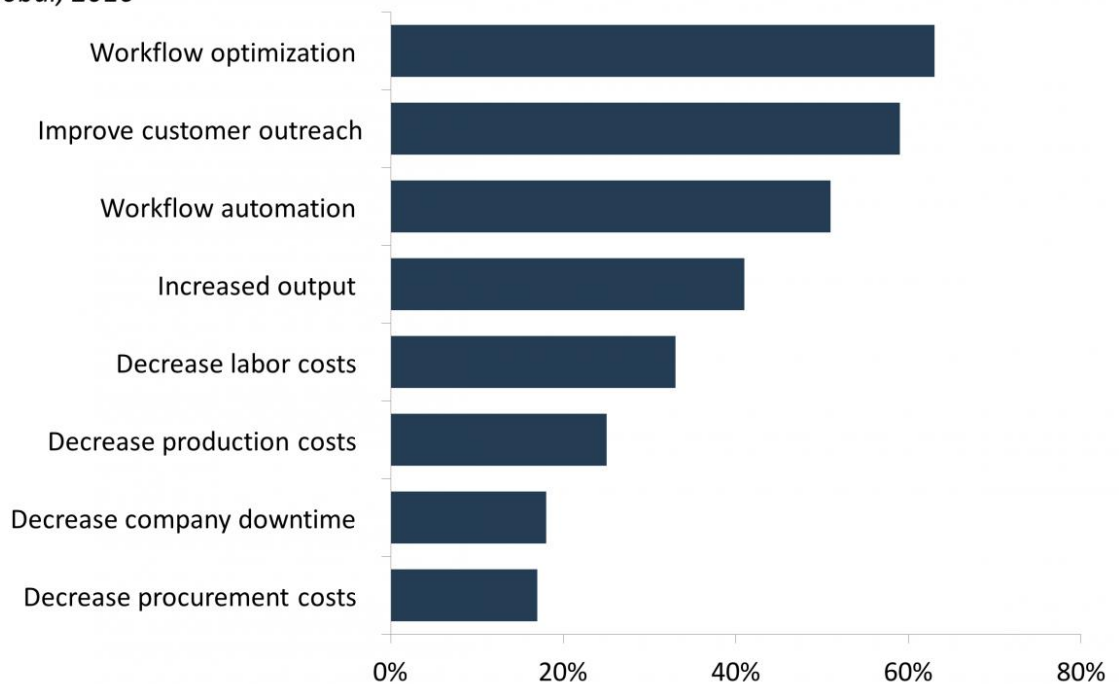


Drivers Of Implementation

For companies to commit to the investments needed to make IoT solutions a reality for their businesses, they must have compelling reasons to put such plans into effect. Those that decide to move forward likely believe they can maximize several benefits of the IoT including workforce optimization, workflow automation, and even increased output.

Drivers That Led IoT Users To Seek Out Solutions

Global, 2016



Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=232 IoT Users)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

Here are the top drivers behind the implementation of IoT solutions:

- **The top driver that led companies to implement an IoT solution was workflow optimization,** according to our survey data. In fact, 63% of companies are using IoT solutions to make sure workflow is running at maximum efficiency. One example of this would be a company using fleet management devices to track where all of their truckers are located.
- **The second most-cited reason companies implemented an IoT solution was to help improve their customer outreach.** For example, a retailer could use beacons to send customers offers and product promotions while in its store. Similarly, a professional sports team could connect players' gear to provide another view of the game to their viewers. This helps drive engagement and foster relationships with customers.
- **The third most-cited reason was workflow automation.** As discussed, automation is the ultimate goal at the end of the five stages of the IoT. However, it will remain difficult to reach the automation stage until the technology that powers the IoT has matured and become specialized enough.

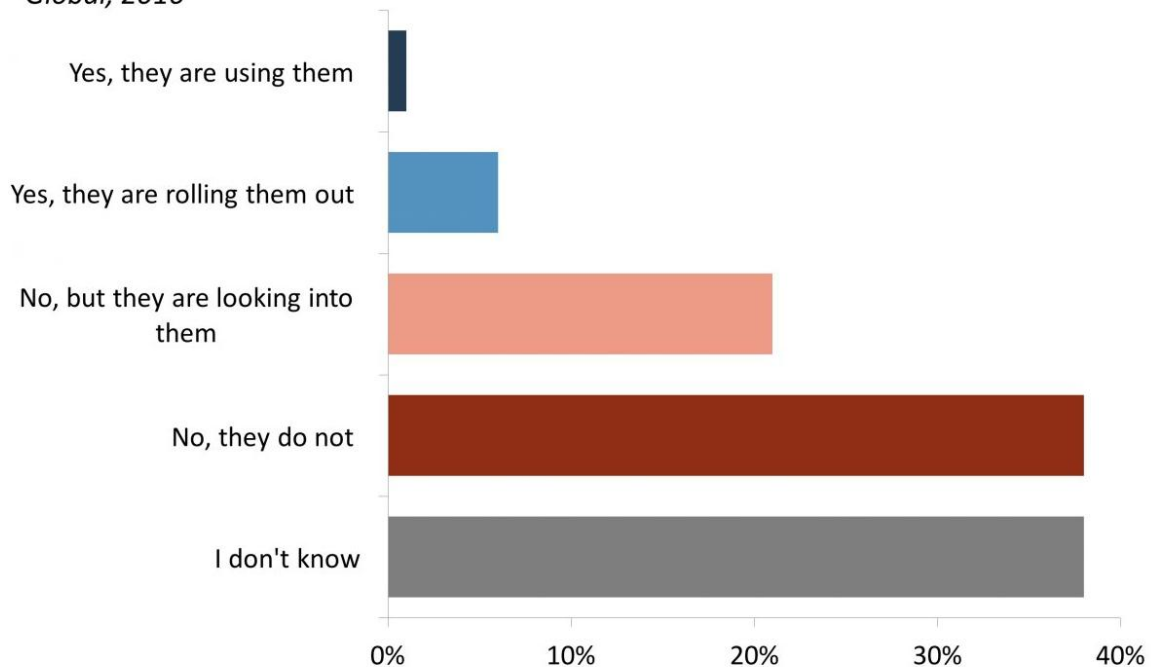
Top Challenges To Implementation

We asked those that had implemented an IoT solution about the top challenges they faced, and similarly asked those that hadn't implemented a solution what barriers kept them from moving forward.

For those that hadn't implemented an IoT solution, the top barrier was that utilizing the IoT did not rank as a priority for management. In addition, only a small portion (7%) of respondents were aware that their company's competitors take advantage of the IoT. Thirty-eight percent indicated that their competitors didn't use IoT solutions, while 21% said they were looking into it. Another 38% were unaware whether their competitors were involved in the IoT. We believe that implementation could have a domino effect on upper management's willingness to adopt an IoT solution. If competitors are already onboard, it's likely that the IoT will be a higher priority for management.

Do Non-Users' Competitors Use IoT Solutions?

Global, 2016



Source: Business Insider Global IoT Executive Survey, Q4 2016 (n=84 IoT Non-Users)
intelligence.businessinsider.com

EXCLUSIVE DATA FROM
BI INTELLIGENCE

For companies that did implement an IoT solution, the top challenge was security.

Connected-device hacks capable of crippling businesses and networks, like the attack on Dyn, are unlikely to be eliminated. And security is a concern that enterprises implementing an IoT solution will continue to grapple with. However, companies wouldn't risk deploying such solutions without the proper security protocols, which means that it's a hurdle each of these firms has overcome.

The second most-stated challenge companies faced when implementing their IoT solution was that the technology had not matured enough yet. For example, an enterprise IoT adopter that needs an IoT solution to analyze the flow of a factory floor and anticipate system failures (i.e., predictive maintenance) will need advanced analytic capabilities to achieve that. That technology might not be perfected, or mature enough, to make a sizable impact on the business.

THE IoT MOVING FORWARD

Regular people are buying smart-home hubs, connected lightbulbs, and other home products. Cities and countries are pouring millions of dollars into initiatives to get smarter and increase efficiency. Stores, factories, offices, and other commercial and industrial workplaces are incorporating sensors and smart platforms to change the way they do business. All of these factors will contribute to the ongoing proliferation of the IoT.

In the year ahead, IoT solutions that combine AI, big data, and automation will continue to gain traction. This sort of system will be especially prevalent and beneficial in manufacturing and industrial settings, where the IoT will allow companies to cut costs by greatly increasing efficiency and reducing the number of employees required to oversee production.

The IoT will further make its way into the mainstream of corporate, industrial, and consumer culture in 2017. Indeed, the next year should see the continued growth and maturation of the IoT, as companies throughout the world continue to seek out, pilot, and fully implement solutions. These new projects will drive growth and propel the total number of IoT devices to 8.4 billion in 2017.

SURVEY METHODOLOGY

Many of the key insights in this report come from BI Intelligence's Global IoT Executive Survey, which was [conducted](#) in September and October 2016 and included over 500 respondents from a wide array of industries, including manufacturing, technology, and finance. Thirty-five percent of respondents came from the C-suite and an additional 27% were in director-level positions, and all were responsible for, involved in, or privy to the IoT decision-making process. A large majority (64%) of respondents were directly responsible for IoT-related decisions at their company.

The study focused on enterprises (41% of the sample representing large enterprise companies with 500 employees or more) who are implementing or planning to implement IoT solutions. The majority of all respondents were headquartered in the US (69%), while the rest of the respondents were international.

Topics covered in the survey include: drivers for adoption; major challenges and pain points; stages of adoption, deployment, and maturity of IoT implementations; investment in and utilization of devices, platforms, and services; the decision-making process; and forward-looking plans.

To learn more about BI Intelligence's proprietary data offerings, please contact intelligence@businessinsider.com.

THE BOTTOM LINE

- The Internet of Things (IoT) is a growing network of connected objects able to collect and share data via embedded sensors.
- The IoT ecosystem is made up of five distinct components: hardware, a network, a remote, a platform, and security protocols.
- BI Intelligence projects that in 2021, the number of IoT devices installed will rise to 22.5 billion, up from 6.6 billion today.
- Companies implementing the IoT are focusing on smaller device installations. Large scale implementations (1,000+ devices) are generally limited to companies with over 500 employees that have the resources and needs to justify them.
- We estimate that annual spending on the IoT will rise from just under \$400 billion in 2016 to \$1.35 trillion in 2021. In total, we expect \$4.8 trillion in IoT spending over the next five years.
- Our exclusive data shows that the majority of IoT implementations at companies surveyed will see total investments of under \$100,000. A multitude of companies will pursue such implementations in the years ahead.
- There are five stages of IoT deployments: connecting devices, managing devices, analyzing device data, creating interoperability between devices, and automating devices. Interoperability and automation are the most difficult to reach.
- The market is largely driven by the technological developments of IoT solution providers, which create, implement, and maintain IoT solutions.
- IoT providers target three broad groups of IoT end users: consumers, governments, and enterprises. The enterprise space is the most targeted by providers.
- The IoT will further make its way into the mainstream of corporate, industrial, and consumer culture in 2017.

BI INTELLIGENCE

BI Intelligence, Business Insider's premium research service, provides in-depth insight, data, and analysis of everything digital. Our research is fast and nimble, reflecting the speed of change in today's business. We give you actionable insights that enable smarter and better-informed decision-making. We publish in-depth reports, news, and an exhaustive library of charts and data focusing on key areas of tech: mobile, e-commerce, digital media, payments, the Internet of Things, and more.

If your organization would like to learn more about our research, including a license to republish our charts, please contact: intelligence@businessinsider.com

Copyright © 2017 Business Insider, Inc. All Rights Reserved.

Proprietary and Confidential Property of Business Insider, Inc.

Licensed for Use By BI Intelligence Subscribers Only.

Access to and use of this proprietary and confidential information is limited by the terms and conditions.