

Sizing Up the Internet of Things



About this Research

CompTIA's *Sizing Up the Internet of Things* research brief provides an overview of key developments of this trend.

This research brief focuses on four areas:

1. Market Overview
2. Internet of Things Ecosystem
3. Business Opportunities
4. Policy and Regulatory Implications

The data for this quantitative study was collected via an online survey conducted during July 2015. A total of 381 U.S. IT companies participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 5.1 percentage points. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimize its influence.

CompTIA is responsible for all content and analysis. Any questions regarding the study should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.

CompTIA is a member of the Marketing Research Association (MRA) and adheres to the MRA's Code of Market Research Ethics and Standards.

Key Points

- New advances in technology have led to strong interest in the Internet of Things, where everyday objects have sensor capabilities, compute power, and connectivity that allows for data sharing. Projections estimate 50.1 billion connected devices by the year 2020 and \$1.9 trillion in global economic value-add, suggesting a world of new opportunity for businesses.
- The ecosystem of the Internet of Things is complicated, spanning hardware, software, rules, and services. Many of these elements have roots in traditional IT components, but there are new aspects to consider and the true value of the system comes from the combination of all the pieces.
- There is a positive outlook for channel firms looking for business related to Internet of Things, since businesses will need help building and applying the complex systems. There will be many new firms focused specifically on IoT aspects such as devices, data analysis, and integration; but there will also be opportunity for channel firms to extend existing offerings into these new areas.

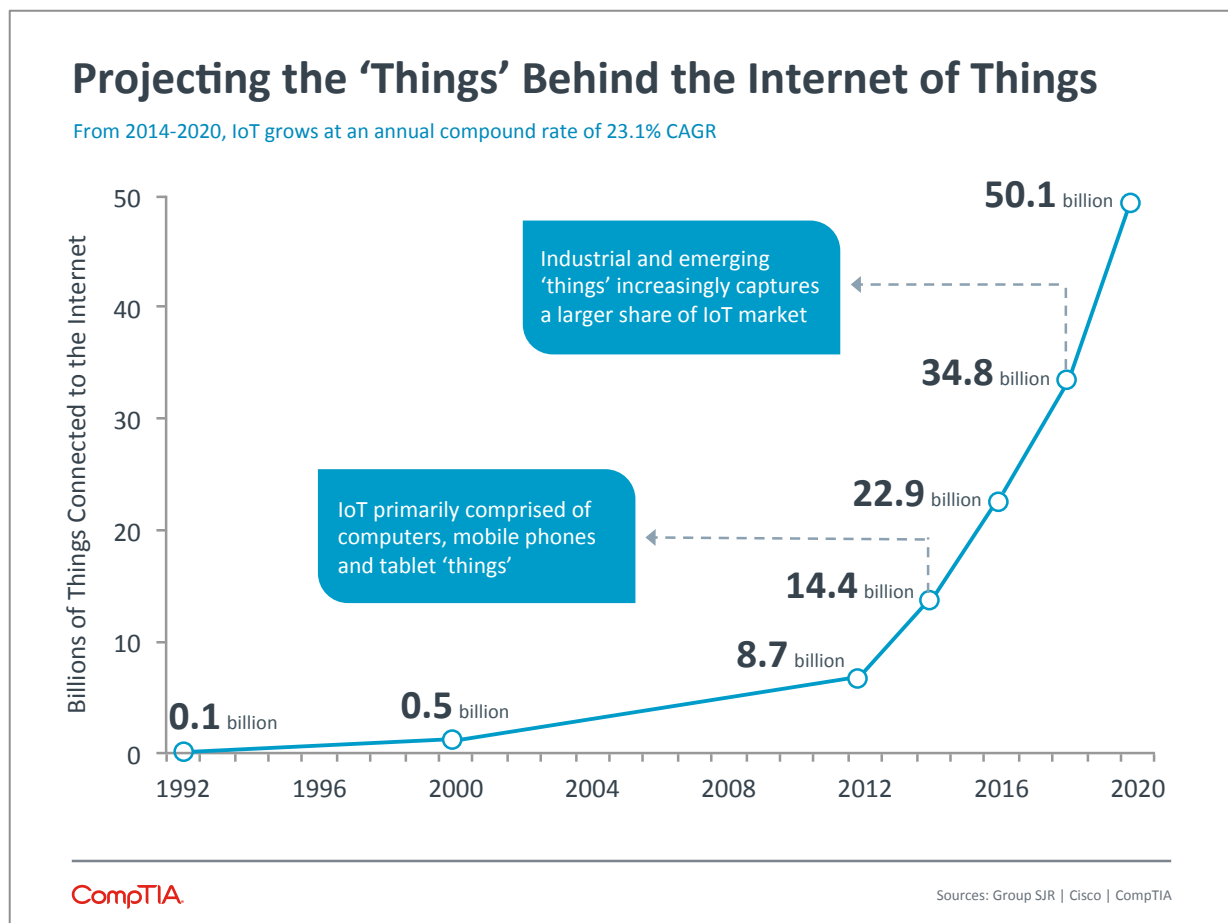
Market Overview

Everything that can be connected, will be connected. This assertion aptly captures the essence of what is known as the Internet of Things (IoT). There is a steady march to enhance the utility of devices, objects, structures and even people through connectivity, network effects and intelligent functionality.

While there have always been ‘things’ connected to the Internet – think computing devices, as well as things connected to other things, such as ATMs, RFID tags or E-ZPass—something has clearly changed. Advancements in a number of areas over the past decade have laid the groundwork for the steepening IoT growth curve. The dramatic rise in computing power and storage capacity offered at ever-lower prices, coupled with the miniaturization of sensors and chips, robust wireless networks, IPv6, and a software-defined world, to name a few enabling factors, make this iteration of the Internet of Things different than prior eras.

The first use of the term Internet of Things is widely attributed to Kevin Ashton, executive director of the Auto-ID Center at MIT, who used it in a 1999 presentation he made to Procter & Gamble. Fifteen years later, definitions and interpretations still vary widely. One simple and concise way to think about the Internet of Things comes from the Oxford online dictionary:

Internet of Things: a proposed development of the Internet in which everyday objects have network connectivity, allowing them to send, receive and act on data. *For more specifics, see ecosystem section of this brief.*



Estimates put the number of ‘things’ connected to the Internet at 50.1 billion by 2020. This translates to approximately 6.3 connected things per person if distributed evenly across the planet. It doesn’t take much, however, to envision scenarios where the per person count is much greater. A connected computer, mobile phone, tablet, printer, TV, media streaming device, watch, fitness monitor, household monitors (security, fire, HVAC, flooding, etc.), car, appliances, and lighting may at some point become common. When adding in businesses or cities and all of the potential areas of connectivity, IoT projections seem quite reasonable.

The count of ‘things’ provides a sense of scope and scale, but that is only half of the story. The revenue side of the equation suggests an equally impressive outlook.

Gartner projects that IoT will result in \$1.9 trillion in global economic value-add – the combined benefits that businesses will derive through the sale and usage of IoT technology. Keep in mind, quantifying value-add benefits, such as time savings or productivity gains is always difficult, with small changes to assumptions often having large impacts.

IDC makes an even bolder prediction, projecting the worldwide market for overall IoT solutions to grow from \$1.9 trillion in 2013 to \$7.1 trillion in 2020. To put into context, the global IT industry, including telecom, reached approximately \$3.7 trillion in 2014. IDC has recently refined this estimate to exclude “intelligent systems”—high-level systems that include IoT components. The 2020 revenue estimate for the remaining core IoT market is \$1.7 trillion. The difference between these two projections further confirms the breadth of ‘things’ that will be part of the Internet of Things. The IT industry undoubtedly sits at the heart of developing, supporting and maintaining IoT, but revenue and value is expected to flow across every sector in the economy.

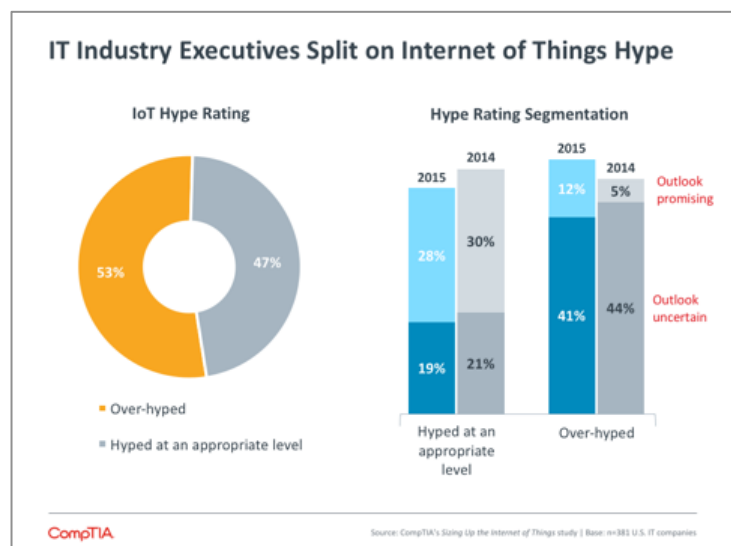
One other forecast: General Electric predicts the [Industrial Internet](#), their interpretation of IoT, to boost global GDP by \$15 trillion over the next 20 years.

If everything falls into place, these lofty projections may very well come to fruition. But, what if everything does not fall into place? How will the inevitable standards battles, security breaches, privacy concerns, monetization challenges, and other unintended consequences affect growth?

A recent survey of IT industry executives conducted by CompTIA confirms these potential inhibitors do indeed raise a number of growth red flags.

Overall, IT industry executives are nearly evenly split on their view of IoT hype. Forty-seven percent of respondents believe the opportunities presented by IoT justify the hype, while 53% see more hype than substance at this point in time.

This is a slightly more negative view than industry execs took a year ago. IoT is likely following the path of most trends in suffering some disillusionment after initial



excitement, especially because the complexity of IoT makes immediate results difficult to come by. While some business cases have emerged, many IoT examples involve consumer applications or do not clearly outline the business opportunities.

As expected, among the segment rating IoT as over-hyped, the majority sees an outlook clouded with uncertainty. This view is especially prevalent among small IT companies, which may be a function of risk aversion or possibly a “here and now” mindset, whereby emerging opportunities are not yet a focus.

Case Studies: A Closer Look at How IoT is Shaping the World Around Us

Collecting New Data in the SMB Retail Space

Swarm is a new startup with a product designed to provide SMB retailers with the data they need to compete against large retailers and online outlets. The venture-backed firm develops technology to track customers at a physical location, whether they are walking by, stopping in, or checking prices against online options.

Salt Lake City-based IT firm Studio 1099 performed a trial installation of Swarm for one of their largest clients, placing devices in the largest and smallest of the client’s five stores. The devices were incredibly easy to install on the network, but the POS integration was a mixed bag. It was simple in the small store (which used LightSpeed), but did not integrate properly with the larger store’s NCR Counterpoint system. Even with products that are meant to plug in seamlessly out of the box, integration issues will likely drive a need for technical specialists.

After the smaller store had gathered data for 36 hours, the Swarm dashboard displayed metrics such as walkbys, total shoppers, transactions, and total revenue. It also provided analytics such as window conversion, return shoppers, in-store conversion rate, and average ticket. Large retailers can often obtain this information through IP cameras or infrared heat tracking, but these systems are not affordable for smaller retailers. Likewise, online retailers have tools such as Google Analytics to easily capture this type of data. An additional feature of Swarm designed to combat showrooming is the ability to track which websites are being visited, giving store owners the ability to directly adjust pricing or speak to the value of an in-store purchase.

Swarm’s low price point gives small retailers an option for gathering data for their store using customers’ smartphones, which can increasingly be used as digital wallets in POS systems. Of course there are security and privacy issues that must be addressed, but these systems along with others such as RFID inventory management allow retailers to digitize their operations more than ever before.

Medication Delivery with a Connected Pharmacy

The Iowa-based healthcare provider Great River Health Systems realized that their processes for medication management were inefficient and error-prone. Manual processes resulted in a medication delivery time of 90 minutes rather than the 30 minutes prescribed by the Centers for Medicare and Medicaid Services (CMS), and the system required three full time technicians to handle inventory and delivery.

Great River implemented a new automated medical delivery system from Omnicell. The connected medication cabinets run on Windows Embedded, provide security via fingerprint scanners, and print patient-specific labels to ensure safe administration. On the back end, a packager and carousel in the pharmacy constantly monitor inventory and automatically place orders to wholesalers when restocking is required.

As a result of these integrated systems, Great River estimates that nurses spend 33 percent less time at medicine cabinets and that interruptions in medication administration have been cut by 54 percent. By reclaiming space and keeping inventory properly stocked, the hospital saved \$400,000 in inventory costs in the first year. Overall, Great River expects to see annual savings of \$300,000 thanks to the decreased labor, inventory reductions, and lower waste that are brought about by the connected system.

Driving Highway Efficiency Through Data

The word 'traffic' in IT discussions usually involves networks and packets, but IoT is allowing transportation agencies and government entities to gather information and make decisions about what is happening on the roadways. Vehicle sensors, intelligent infrastructure devices, and social streams can all be combined to provide a view of traffic flow and help alleviate congested areas.

Pulling all this information together highlights the Big Data aspect of IoT. There is a tremendous amount of data, different data is structured in different ways, and analysis has to be done quickly in order to inform further decisions. Collecting the data and performing analytics may be a natural extension for IT solution providers who deal with storage or databases, though new skills and tools will likely be needed.

An example of a new tool for traffic management is the SmartCity StreamApp. This data management application from software developer SQLstream is a basic platform that can be configured for the needs of different clients. Various data streams can be connected as inputs, then the application can be integrated with existing traffic management systems to automate congestion management or provide real-time travel times. The SmartCity StreamApp is not a new type of intelligent device in IoT, but instead is a new software platform that brings together data from intelligent devices in a useful way.

Building Smarter Cities

Traffic planning is just one aspect of the huge efforts taking place to make cities more predictable and efficient. Smart city projects can also involve parking, utility consumption, structural health of buildings and bridges, lighting, and waste management.

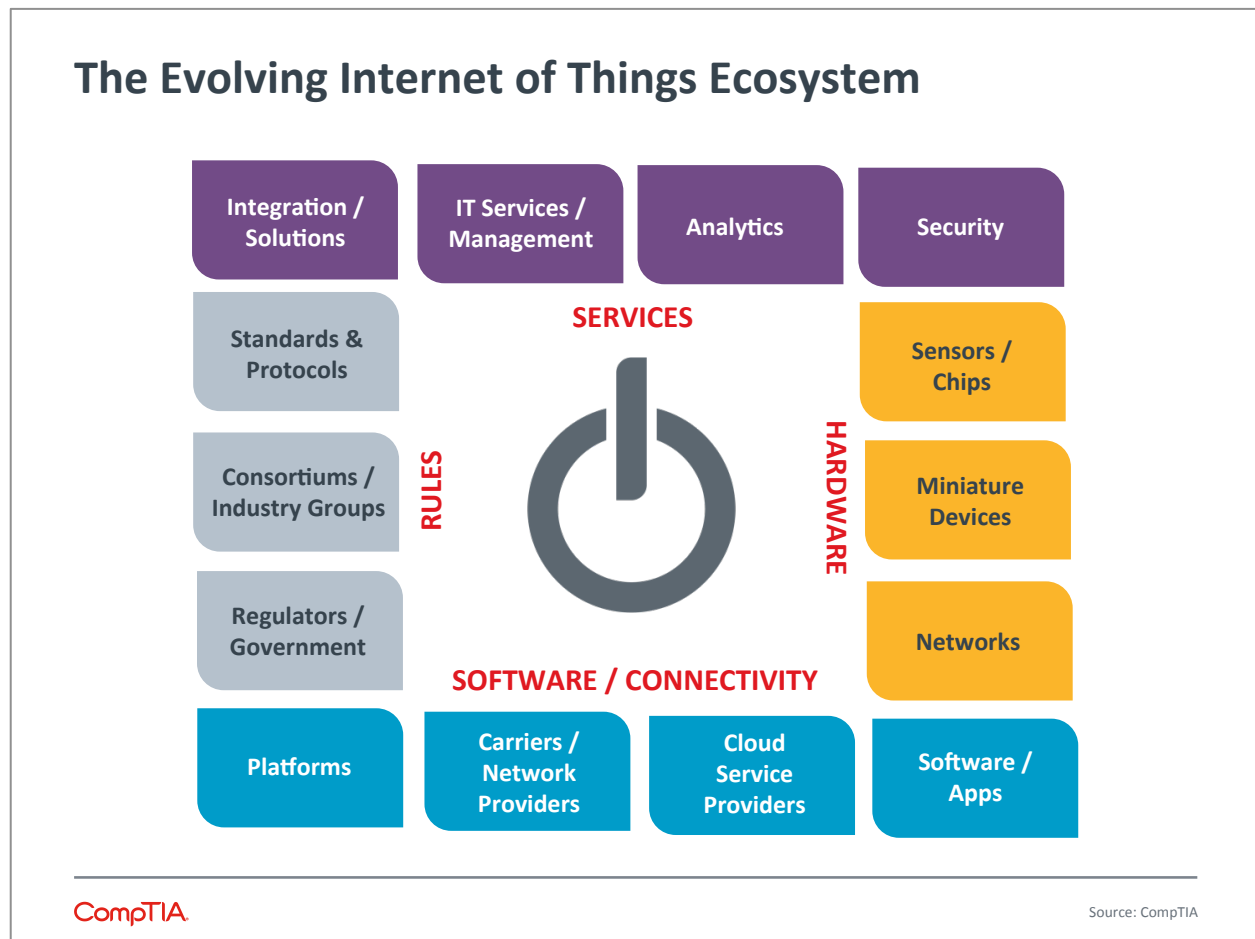
One of the earliest adopters of a comprehensive smart city initiative was Dubuque, IA. Working in conjunction with IBM, this 60,000-person city began taking steps to modernize its infrastructure, become more sustainable, and take steps forward into a connected future.

The initial step in Dubuque's planning illustrates the broad scope that IoT projects typically entail and the work required to start things on the right foot. Starting from a platform of sustainability, city officials worked with a broad range of constituents, including residents, government representatives, business owners, and community organizations. Buy-in from all these groups was important as they needed to understand the technology being implemented and the data being collected.

With a plan in place, the process of installing sensors and networks began. Rather than overhauling multiple systems, Dubuque started with a project already underway—the replacement of water meters. Through a 15-week pilot, the technology team was able to learn about integrating technology with the physical world, building a robust backend to handle all the data, and providing an interactive frontend to consumers to deliver real-time information.

The water system pilot proved successful, leading to a 6.6% reduction in household water consumption and a significant increase in leak detection. An electricity program soon followed, and pilot households found that their electricity usage decreased by 11%. Subsequent projects led to more efficient public transportation, greater economic development, and global recognition as an early leader in smart city development.

The Internet of Things Ecosystem



As with most recent trends in technology, the Internet of Things is composed of many different pieces working in concert to create a new model. IoT is a perfect example of the developments referenced in a recent McKinsey and Company paper on digital transformation: “The digital technologies underlying these competitive thrusts may not be new, but they are being used to new effect.”

Although ‘Internet of Things’ may not be the catchiest name the industry could have chosen for this trend, it actually is a fairly good reflection of the composition of the underlying ecosystem. Just as the traditional Internet has many different components and is not a discrete product, IoT has many pieces that must be understood at a basic level in order to build value-added services.

Hardware

Hardware, including the ‘things’ in IoT, is the first piece of the puzzle. Advances in miniaturization and the low cost of high performance silicon (as dictated by Moore’s law) have led to both sensors and compute components that can affordably be placed in practically any type of device. Inexpensive sensors can measure everything from geolocation to temperature to blood pressure and translate this information into a digital format. Computing can be done onboard in many cases, or the data can be transmitted to a central compute location.

The type of device that might contain this capability is practically limitless. At one end of the spectrum are extremely large devices such as cars, which are soon expected to carry over 200 sensors each. At the other end are devices such as the Michigan Micro Mote, which packs processing, data storage, and wireless communications into less than a cubic millimeter. In between are any number of objects that have never before had compute capability or connectivity, and the vast majority of these will come from vendors that have not traditionally been part of a technology solution.

A final piece of hardware to consider is the network. With so much data being transmitted, robust networks will be a critical part of any strategy around IoT; in fact, much of the momentum behind the trend has been generated by producers of networking equipment. The need is very real, though—CompTIA research consistently shows that unplanned network upgrades often contribute to the hidden costs behind new technology implementations.

Software/Connectivity

On its own, a collection of chips and sensors has limited use. Software is required to tie everything together or make the data usable, and connectivity is required to share information or communicate with the entire system.

The software component begins with new platforms. The primary example of this is the new operating systems that have dominated the mobile device landscape. During the PC/Internet 1.0 era, Microsoft Windows was the dominant OS, especially in terms of front-end or consumer computing. With smartphones and tablets, iOS and Android have become major players. As consumers expand their notion of computing to include wearables, homes, and cars, different vendors are also seeking to expand their operating systems into those areas.

Aside from the operating systems, there is a firmware of sorts needed for IoT to be successful. This firmware itself is made of multiple components. As the cloud is a primary tool in facilitating IoT, the software by cloud providers to construct their offering plays an important role in the overall solution. This software is made available to other parties through APIs, which will be dependent on both the cloud software and the access a cloud provider is willing to grant.

Many companies that have traditionally operated as telecom carriers are looking into providing cloud solutions as well, and these offerings could be of interest if they are packaged with broad network capabilities. Cellular and Wi-Fi networks have enabled modern computing models, but they also come at a cost that must be considered when building a plan around new data streams.

Rules

Hardware, software, and connectivity make up the technical foundation for IoT, but there is another major element that will dictate the way the subject develops. Standards, regulations, and best practices will shape the way that companies implement projects, and several different organizations are involved in helping build these rules for IoT.

Many industry observers view standards as the largest hurdle to mass adoption. This, of course, is typical whenever a new technology format or model is introduced. Betamax/VHS and HD DVD/Blu-ray are popular examples of standards battles that eventually produced a clear market leader. The IoT standards discussion will most closely resemble the development of the TCP/IP model that enabled the

traditional Internet to become ubiquitous. The discussion is less about a winning format and more about overall function and usability.

Just as TCP/IP encapsulates several networking layers (link, internet, transport, and application), a standards model for IoT will need to address several areas. IoT layers will include connectivity (where cellular networks and Wi-Fi networks must be combined in optimal ways), data transport (where TCP packets may need to be modified to account for network constraints), and devices (where power consumption concerns will drive practices). New protocols such as 6LoWPAN, Constrained Access Protocol (CAP), and Time Synchronized Mesh Protocol (TSMP) will be introduced throughout the ecosystem as the various layers need to interact with each other.

The technical side is just one half of the challenge in successfully building IoT systems. The other half is in dealing with social concerns, such as the security and privacy implications inherent in mass numbers of connected devices sharing data. Here, there will likely be government action, building on regulations that have been established to cover activities such as electronic health records or digital collection of financial information.

Services

Services are typically not considered to be part of an ecosystem; instead, they are built at a higher layer to combine foundational pieces into a cohesive offering or to simplify the solution for an end user. This is partly the case with IoT, but there is also an argument that services are more tightly ingrained into the basic ecosystem.

Choosing Sides

Many organizations have formed in an attempt to define standards for IoT. As of August 2015, five groups are demonstrating strong momentum. Some companies are throwing their full support behind a single endeavor, while others are participating in multiple groups in order to be well positioned as the landscape shifts.

- **AllSeen Alliance:** One of the first groups to form, AllSeen has used Qualcomm's AllJoyn device interconnect framework as a foundation. Other members include IBM, Cisco, Microsoft, and LG.
- **Open Interconnect Consortium:** Driven by concerns over Qualcomm's interests in promoting AllJoyn, the OIC is seeking a more ground-up protocol creation. Members include IBM, Intel, Dell, and Samsung.
- **Thread:** Thread is another ground-up effort to create a networking protocol with better security and low-power features than Wi-Fi, NFC, Bluetooth, or Zigbee. Members include Nest (a division of Alphabet), Samsung, ARM, and Freescale.
- **Industrial Internet Consortium:** The IIC is focused on bringing connectivity and intelligence to industrial applications. Members include GE, IBM, Intel, AT&T, and Cisco.
- **Wireless IoT Forum:** This group has a particular focus on spectrum, with a goal to drive standards and counter fragmentation in licensed and unlicensed wireless M2M market. Members include Cisco, Arkessa, Telensa and WSN.

While the IoT ecosystem consists of hardware, software, and rules, the true value lies in the data being generated, captured, and analyzed. This data does not hold much value on its own without services that perform the analysis and present findings or insights in a useable way. Additionally, the data has to be highly available and tightly protected.

The complexity of IoT is another factor that drives a critical need for services. Standards and protocols will help create some conformity, but the reality is that there will still be multiple systems interacting. Consider a smart home, where HVAC, lighting, and home entertainment (among others) will generate data that a homeowner will want centralized for control. That central control will likely need to be available on a variety of different platforms—PC, tablet, and smartphone. Even with standards in place, creating this comprehensive system is a complicated task.

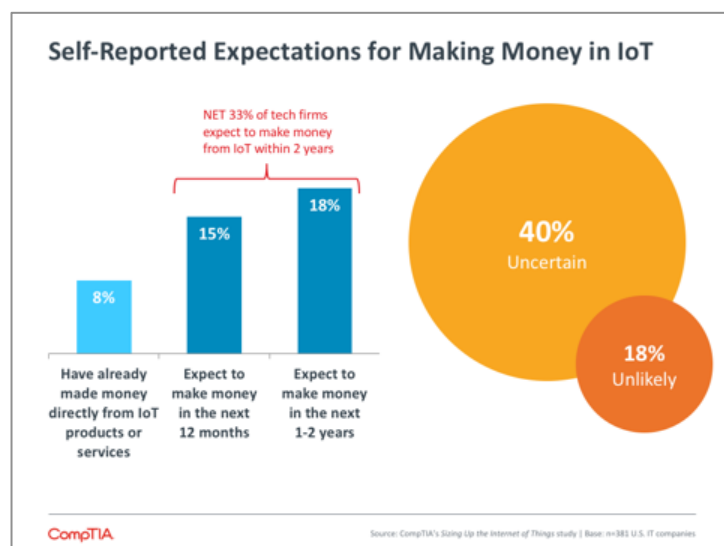
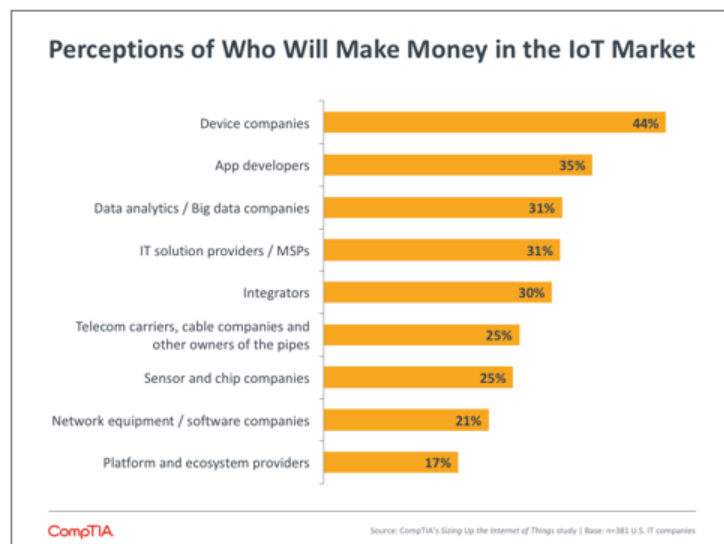
Services, then, are an important ingredient in realizing the full benefits of IoT. Whether the service is at a higher level dealing with data and integration or at a lower level dealing with infrastructure, there are many opportunities for channel firms to build offerings around this new trend.

Business Opportunities

With any new technology, one question always rises to the forefront: How do you make money? This is especially important for established companies, as they must compete with focused newcomers while maintaining their existing revenue stream.

For IoT, the threat of newcomers is certainly in play. The top three company types that IT executives imagine making money from the new trend all have a specialty focus that applies directly to the technology. Of course there are device manufacturers, app developers, and data analytics services in practice today. The difference is in the construction and demands of the devices, the structure and speed of the data, and the software and APIs that are used for integration.

This is not to say that there will be no opportunity for other firms in the IT or telecom channels. After these IoT-specific companies, IT solution providers and MSPs are next in line when it comes to profit expectations. The primary dynamic that fits the business model of



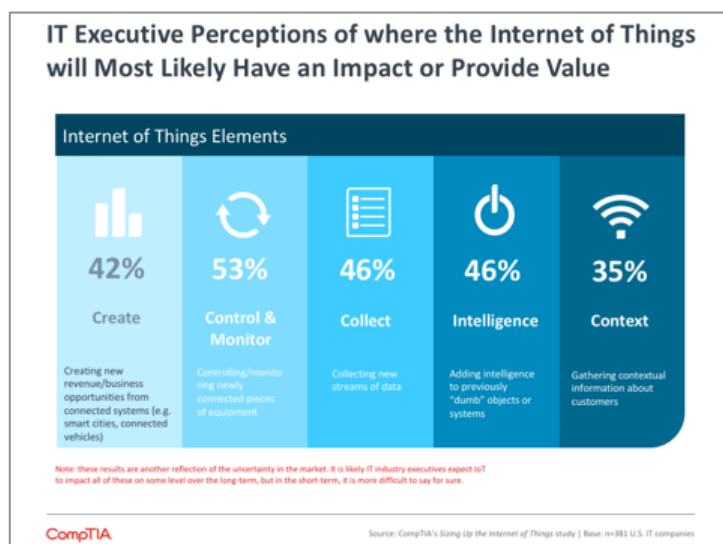
these firms is complexity. The growing complexity of IT has led to more demand for managed services, and the inherent complexity of IoT will drive businesses to seek help in extracting value from the systems.

As solution providers aim to reduce complexity for their clients, they will need to build up their skills in dealing with IoT technology. This may not require drastic change, though. Many areas of IoT can be seen as extensions to skills or lines of business that solution providers already have. In fact, many disciplines that top the list for profit expectations tie back to existing channel fields.

- Devices:** Most break/fix or device management efforts today are focused on office equipment such as PCs or printers, but the same skills and considerations can apply to new devices and sensors. There will be some new areas to consider, such as power usage, security, and network protocols. However, the general business processes for device repair and upkeep will be applicable, as will any experience in monitoring connected devices.
- Data Analytics:** While the data streams generated by IoT devices will require new data warehousing techniques and new analytics tools, these new functions are often complementary to existing techniques and require a strong foundation in data management. CompTIA research has found that many companies, especially in the SMB space, do not have this foundation. These companies can benefit from data audits along with more traditional tools such as SQL or relational databases before moving into new areas.
- Integration:** As with data analytics, many channel firms are already providing integration services. These firms recognize that integration typically constitutes the bulk of the effort for a new IT product and have built the planning practices necessary for integrating complex systems. The new skills required for IoT integration will be the APIs that connect various devices and services, especially as standards are in flux.

One standout discipline is application development. This is an area where channel firms are typically not as strong, but it has become critical for driving mobility initiatives. Business applications often need a mobile-optimized front end in order to produce the greatest benefit, and if a company is using customized legacy software, the front end requires customization as well. IoT applications require a similar front end for simplifying tasks and presenting actionable data insights, so solution providers must begin thinking seriously about how to build mobile app skills or partner with development firms.

Channel firms will need to apply their technical knowledge to their clients' business situations. Aside from any hype associated with the term, IoT presents the prospect of entirely new activities within a company. Businesses will not just be applying new technology to old processes; they will be exploring innovative areas and searching for the



best applications for their specific purposes. Here, the challenge for channel firms is the same one that exists with IT in general—going beyond being a simple supplier and becoming a partner that understands business objectives and uses technology to achieve goals.

IoT Spurs Regulatory Debates

As the Internet of Things moves rapidly from concept to reality, questions surrounding the government's role in this emerging market become more pressing. Eye-opening incidents involving hijacked cars, zombie refrigerators, or hacked radiology equipment have already made the headlines.

It is only a matter of time before even more dire scenarios play out. Imagine a hacker taking control of a heart pacemaker, an airport or a stock exchange to wreak havoc, steal IP or demand a ransom. Perhaps slightly less egregious, but no less concerning, imagine getting a notice from your insurance company expressing concern over your two visits to a fast food restaurant last month or your three instances of speeding. There are countless other scenarios, many seemingly out of science fiction movies, that will test IoT stakeholders on multiple fronts.

IoT is now a top of mind issue for regulators and policy makers in the U.S. and abroad. To date, the U.S. Senate, the House of Representatives, the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the EU Commission, as well as other industry bodies, have held hearings or discussions addressing some aspect of IoT (see Appendix for details). Discussions tend to revolve around several fundamental elements of IoT:

Security

Security tops the list of IoT policy concerns. With the projected growth of connected devices and the corresponding increase in potential vulnerabilities, especially in new domains such as critical infrastructure, the security component of IoT provokes a number of thorny questions. For example, could security flaws be classified as product defects, making connected cars or appliances subject to recalls? Could support and service firms, such as IT solution providers, electricians, or mechanics, be held responsible for security incidents? Could corporate boards of directors face liability?

The FTC whitepaper, [*Careful Connections: Building Security in the Internet of Things*](#), outlines key considerations and best practices for securing IoT. This includes not only the need to build robust security safeguards into IoT devices and systems at the earliest stages of development, but also ensuring ample resources are devoted to providing guidance and training to all types of users, whether they are consumers, small businesses, city employees or multinational corporations.

Data Privacy

Closely related to security is the issue of data privacy. Most users of technology are not fully aware of the extent to which their personal data is collected, bought, sold and used by various parties. This could be considered the tip of the proverbial iceberg. In a hyper-connected IoT world, the depth and breadth of data privacy concerns will greatly exceed those of today. Of course, many users willingly hand over certain data in return for access to services or capabilities. Issues related to acceptable use, opt in vs. opt out, right to be forgotten, data breach notification, data ownership, customer privacy bill of rights, and cross-border legalities will be of particular interest to regulators.

Spectrum and Standards

While it is impossible to know exactly how the IoT market will evolve over the next decade, it is fairly certain that IoT advances will strain existing spectrum allocations as billions of new wireless IP devices come online. When a mobile phone drops a call, it is chalked up as an annoyance. Should a driverless vehicle lose its connection, the consequences could be far more severe. The FCC is currently working to set rules for a 2016 auction of spectrum now used by broadcast television stations. Interest in this block of spectrum will be high due to its suitability for sending mobile broadband signals over long distances. Beyond commercially licensed spectrum, the FCC will also need to continue to evaluate options associated with unlicensed or white space spectrum – bands used by Wi-Fi or Bluetooth, for example.

As covered previously in this paper, standards play a pivotal role in ensuring interoperability and efficiency in the IoT ecosystem. Historically, many standards and protocols in the tech space emerge from industry-led efforts, typically in conjunction with ANSI or ISO. In some cases, the market can support multiple competing standards; while in others, a single standard ultimately takes hold. IoT consortiums, trade associations, standard setting bodies, and companies with sufficient clout will continue to hammer away at establishing a market-optimized set of IoT standards and protocols.

Commerce

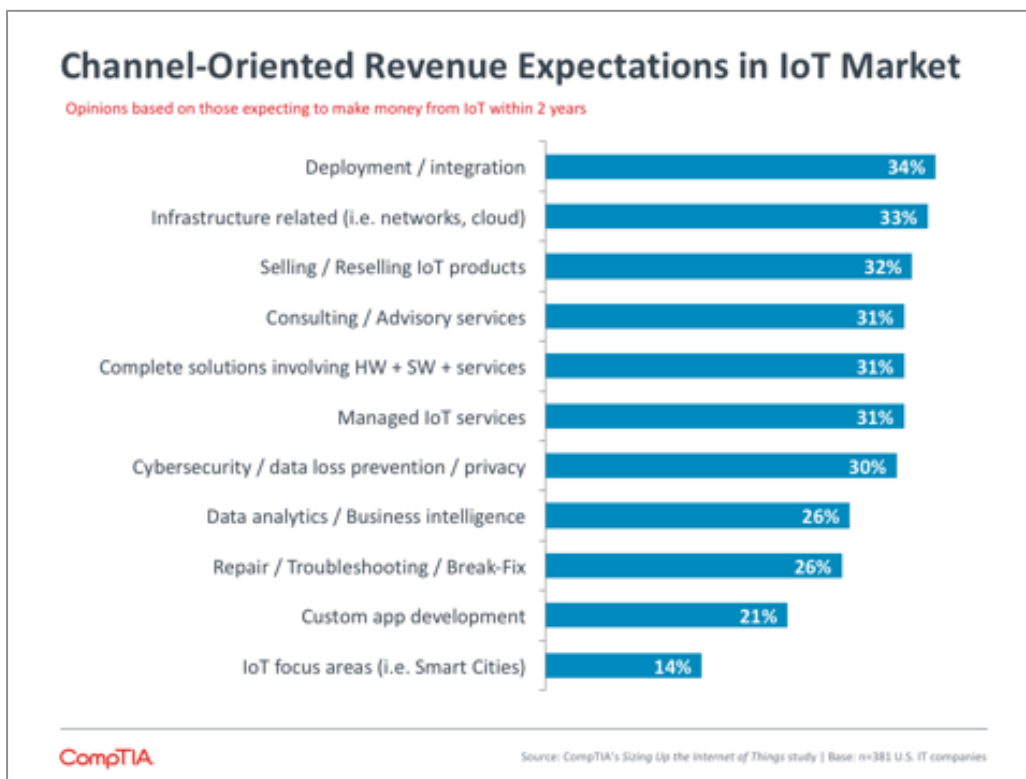
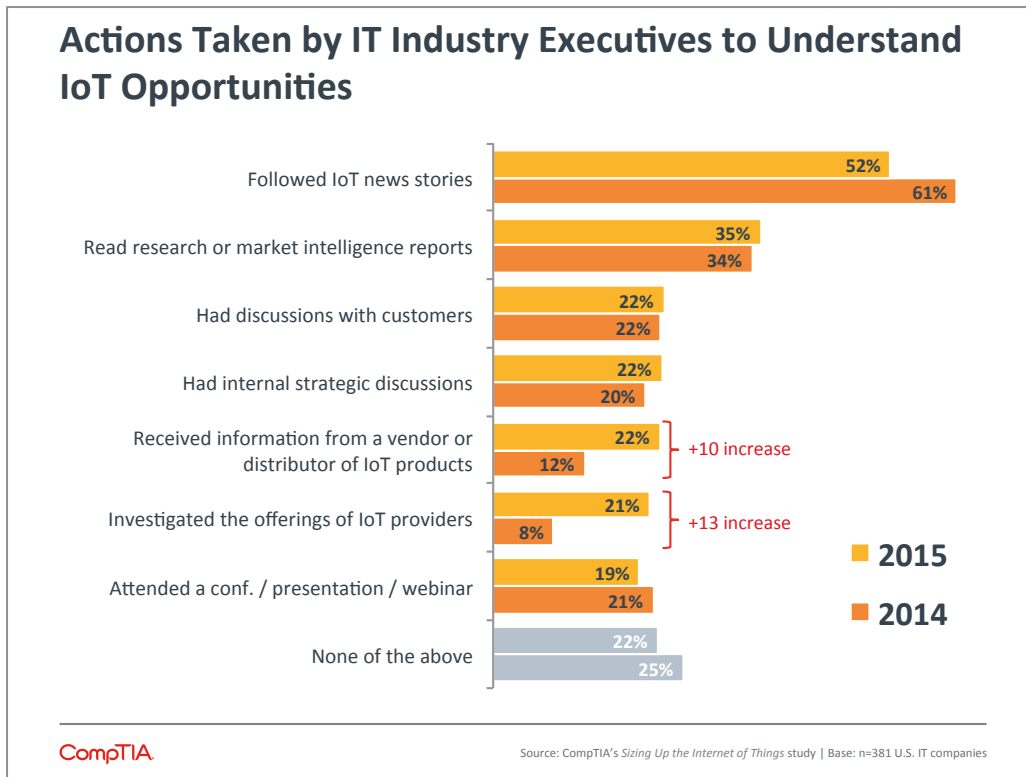
The intersection of IoT and commerce has not received as much attention as other higher profile issues, such as security, but there are a number of policy questions in this arena that will require attention. Consider the issue of data ownership. It is not always clear who owns what. Do households own the detailed usage data from water, gas and electric meters, or do the utility companies own it? Additionally, what are the rules that govern third party access to this type of data through APIs? Debate is underway in states such as Illinois (see [Illinois Grapples with Question of Who Owns Energy Data](#)) to sort through these issues, which have potentially far reaching implications for IoT commerce.

Another interesting issue involves taxation. In most cases, IoT products and services will fall under existing tax law. But, could IoT facilitate new ways to assess or collect taxes? Could a cash-strapped state decide to impose a tax on certain types of IoT commercial activities? Could a foreign government impose restrictions on U.S. IoT providers which act as an import tax? These scenarios will undoubtedly spur intense tax policy and commerce debates.

Public-Private Partnerships

One of the more compelling visions for IoT centers around improving the foundational systems that support cities. Electric grids, transportation networks, food production and public services could all benefit from greater intelligence and machine-to-machine or machine-to-human interaction. Often referred to as smart city initiatives, there are quite a few pilots taking place in cities around the world, many of which entail public-private partnerships (see Building Smart Cities callout above or examples at the [Smart Cities Council](#)). These may take the form of allowing an IoT provider to embed sensors in city-owned infrastructure or building mash-up services on top of government data sources. In more advanced applications of IoT involving ‘systems of systems,’ such as connecting transportation, weather, and financial systems, public-private partnerships will be essential to maximizing the benefits to citizens, businesses and government entities.

Appendix



Examples of Public Policy, Regulatory or Trade Associations Engaged in IoT Discussions

Federal Trade Commission (FTC)

[*Internet of Things: Privacy and Security in a Connected World*](#)

U.S. House of Representatives Energy and Commerce Committee

[*The Internet of Things: Exploring the Next Technology Frontier*](#)

U.S. Senate Committee on Commerce, Science, and Transportation

[*The Connected World: Examining the Internet of Things*](#)

European Commission Alliance for Internet of Things Innovation (AIOTI)

<https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti>

CompTIA New & Emerging Technology Committee

<http://www.comptia.org/advocacy/policy-issues/new-emerging-tech>

IEEE IoT Technical Community

<http://iot.ieee.org/>