

2019 TRENDS IN INTERNET OF THINGS

February 2019

Internet of Things is another trendy buzzword in the technology industry, and companies have been trying to determine how much is hype and how much is reality. The promise of new data streams or a higher degree of automation is certainly tantalizing, but the greatest benefit comes from large interconnected systems that present a challenge for many organizations. An Internet of Things strategy requires new technology along with new business processes and collaboration. This study explores how companies are navigating the early stages of adoption, including financial considerations, technical skills, and potential partnering.

KEY POINTS

Internet of Things has a broad ecosystem

While the initial impression of the Internet of Things trend may be about the “things,” there is more to IoT than just hardware. Software plays a key role connecting all the devices and orchestrating activities. Rules and standards will enable mass adoption. Services will provide access to benefits for those firms that choose not to focus on building their own systems. Few companies feel they have high expertise in any of these areas, so integrating them all together will obviously provide a significant challenge.

Internet of Things initiatives span the entire business

Rather than being standalone IT projects, 63% of companies with current IoT initiatives say that they are incorporating IoT technology into existing business processes. This makes IoT a clear example of digital transformation, where companies are recognizing that simply bringing in new technology is not enough; there has to be a methodology for bringing together the technical skill of IT with the business acumen of various departments. This understanding must start at the executive level in order for collaboration to succeed.

Financial implications are difficult to calculate

Although 35% of companies view IoT through the traditional IT lens of cutting costs, 31% take the view that IoT can help drive new revenue. This could be done by increasing production, monetizing data, or creating a product-as-a-service offering. With different possibilities for the financial return and multiple areas of investment needed, 58% of companies say that determining ROI is “very difficult” or “moderately difficult.”

Internal and external skills are needed for success

IoT-specific roles such as IoT Architect or IoT Security Specialist are not the only things companies should consider as they are trying to close their skill gaps. Improvement is often needed in foundational areas, such as security, networking, and cloud computing. Small companies in particular may not have the ability or desire to build all these skills in-house, so expanded partnering will likely be a part of IoT strategies. In terms of the IoT ecosystem, more companies use a third party for software (83%) than any other area.


MARKET OVERVIEW

Given the staggering number of technology innovations that have been introduced recently, it is difficult to say which one claims the top spot as the most disruptive. Smartphones completely changed the perception of where computing could take place. Cloud systems created a new mindset around how computing could be utilized. Artificial intelligence is expanding the definition of what computing is capable of. But it may be that Internet of Things is more disruptive than any of these, as it reinvents what computing even is.

Moore's law, improved manufacturing techniques, and ubiquitous connectivity have all contributed to the basic premise of IoT: every physical object can now become a digital device, able to capture data, perform computations, and connect to a network. As Microsoft's CEO Satya Nadella said in 2018, "The world is becoming a computer. Computing is becoming embedded in every person, place, and thing."

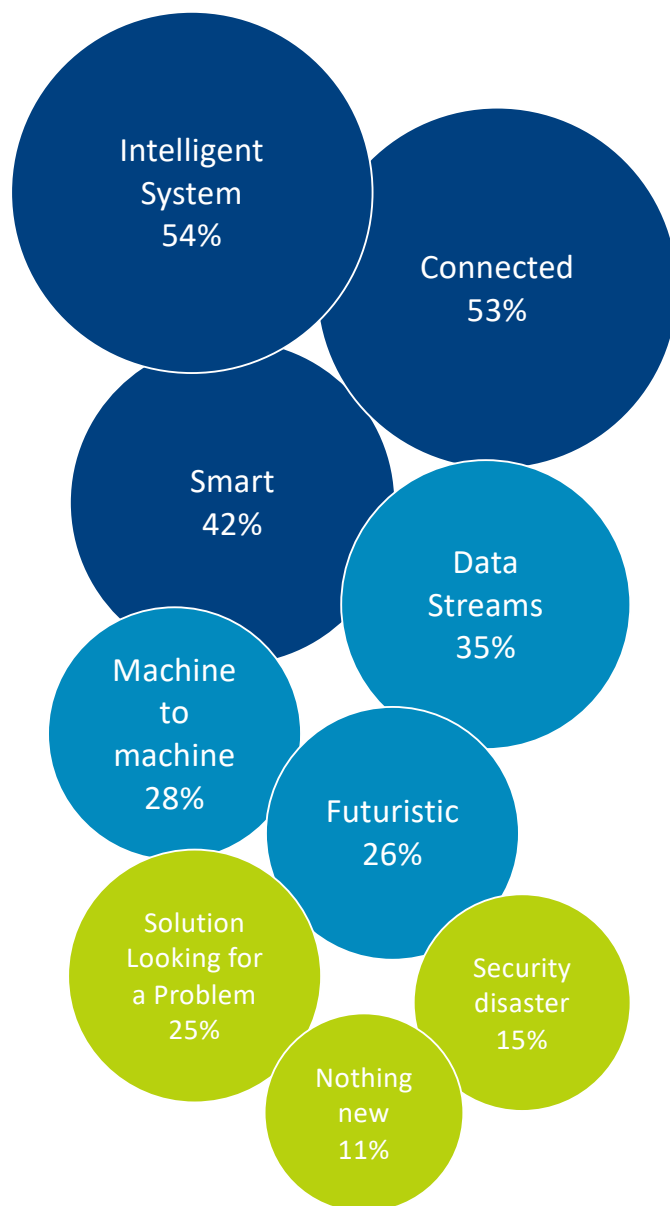
One of the most popular approaches for describing the extent of IoT's impact has been connected devices. The numbers are eye-popping but not always consistent; early projections by Cisco showed 50 billion connected devices by 2020, while early projections by Gartner only showed 24 billion connected devices in the same timeframe. As with any projections, the numbers are in a constant state of flux, and they likely miss the point anyway. At some point, there are simply enough connected devices to force new behavior. Furthermore, each organization will build its own behavior as it drives a strategy around devices and data.

Projections for revenue are just as varied as projections for connected devices, but they still provide an additional lens for viewing the impact of IoT. The research firm Bain & Company predicts that global IoT spending will reach \$520 billion in 2021, and IDC estimates global IoT spending to hit \$1.2 trillion by 2022. For context, IDC reported that overall IT spending worldwide in 2018 was \$4.5 trillion. IoT-specific spending is not likely to be a quarter of all IT spending, so IDC's IoT number includes items needed for IoT that typically fall into other categories, such as networking equipment or database software.

This range, though, is a good representation of the far-reaching nature of IoT. Rather than being an isolated product that is installed alongside other IT components, IoT is a strategy that relies on many parts of the IT infrastructure. In fact, most companies see a strong or moderate connection between IoT strategies and other technology initiatives within the organization, especially cloud computing, mobile devices, and artificial intelligence.  **FURTHER READING**

The overall perception of IoT is positive and has mostly held steady over the past few years. There are a few notable shifts. In 2016, just 40% of IT and business professionals associated the term "intelligent system" with IoT. Today, 54% of IT and business professionals make this association, placing it at the top of the list. It's encouraging to see a trend towards this

Terms associated with Internet of Things



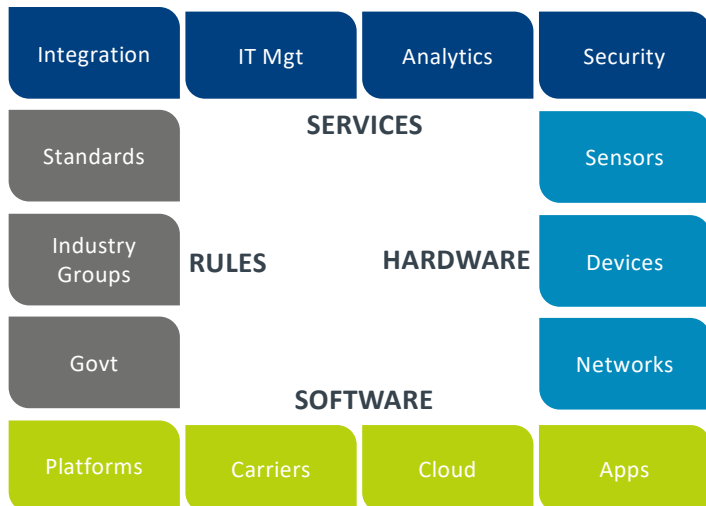
term rather than the simpler "smart." Certainly the implication of computing capability and decision making is still there, but "intelligent system" also includes the notion of many connected pieces working in concert.

On the other end of the spectrum, there has been a drop in the number of people who perceive IoT as nothing new, as merely an extension of the internet. Those that have been paying close attention to the IoT space recognize the immense potential in bringing some of the connected concepts of the internet to physical objects that have previously had no computing capability. There are clearly some risks to be considered in such an expanded concept, but the potential to be gained from analyzing new data streams and automating environments is something every business should be pursuing.

UNDERSTANDING THE COMPLEX IOT ECOSYSTEM

It's no big surprise that a field as far-reaching as IoT has a complex ecosystem. Even at a basic level, there are many pieces—both technical and non-technical—that must be tied together for a successful IoT implementation.

The evolving IoT ecosystem



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. Building robust networks for this data transmission is another part of the hardware equation.

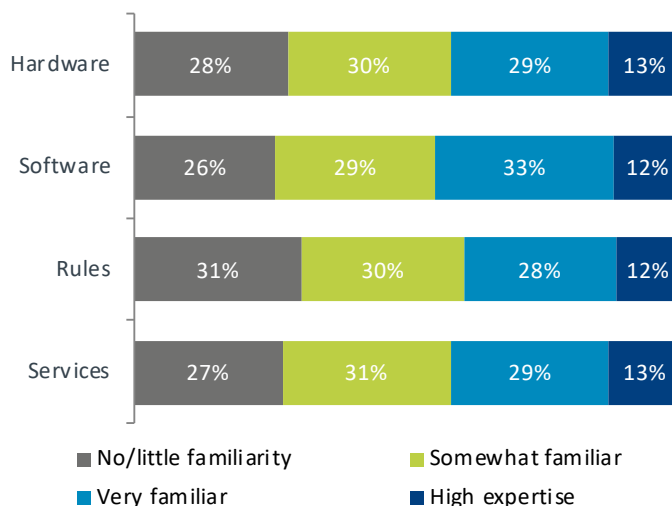
The software component begins with new platforms. The primary example of this is the new operating systems that have dominated the mobile device landscape. During the PC/Internet 1.0 era, Microsoft Windows was the dominant OS, especially in terms of front-end or consumer computing. With smartphones and 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 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.

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. 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.

Familiarity with ecosystem elements



Are businesses ready for this degree of complexity? Looking at levels of familiarity across each part of the ecosystem, it appears that there is some work to do. Very few companies claim to have the highest level of expertise in any area. In some cases, they may be selling themselves short. For example, the networking and back-end pieces of hardware needed for IoT are likely just extensions of equipment that is already in place. The hardware domain is not exclusively made up of brand new devices.

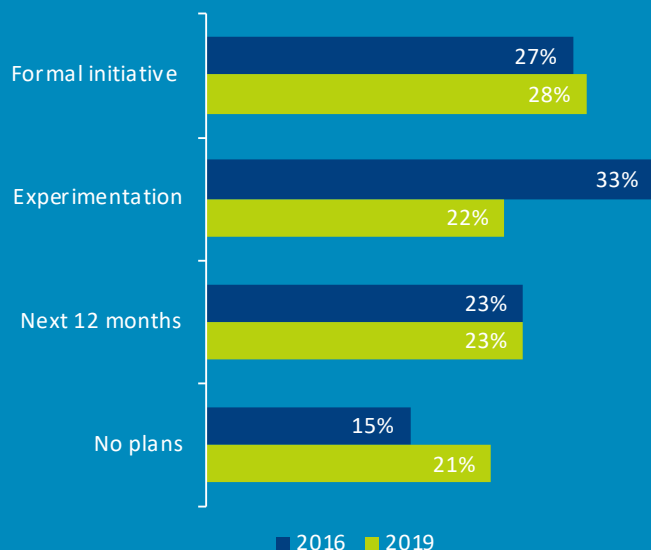
On the other hand, closing gaps across all four ecosystem domains is a large undertaking, and companies will need to think carefully before making IoT investments. Those investments should account for the impact to the business, the skills needed for IoT success, and the partners that contribute specialized expertise.

GETTING STARTED WITH IOT

There has not been dramatic progress in IoT adoption over the past few years. IoT is still the most widely adopted technology in CompTIA's emerging tech tracking, but there are still only formal initiatives taking place at just over a quarter of all companies. The pace of IoT adoption may seem somewhat surprising given the rapid adoption of cloud computing and mobile devices, but there are reasonable explanations for the inertia. Looking at the extended history of technology adoption, it is more likely that cloud computing was an outlier and that adoption patterns will somewhat regress towards typical levels. Furthermore, many emerging trends build on cloud computing along with other components, and the complexity can be a lot to handle, even for companies that are pushing the envelope with technology. [FURTHER READING](#)

The complexity of modern trends highlights an important distinction. The connection between "strategy" and "product" in IT is becoming less direct. Consider a trend as recent as virtualization. There was little difference between having a strategy of virtualizing resources and implementing the products to enable virtualization. More and more, technology strategies go beyond a singular product. Internet, cloud, and now IoT are all examples of strategies that require modified workflows, interdepartmental communication, and a full suite of products in order to be fully realized. Measuring adoption for these broader strategies can be somewhat difficult as companies build all the necessary components.

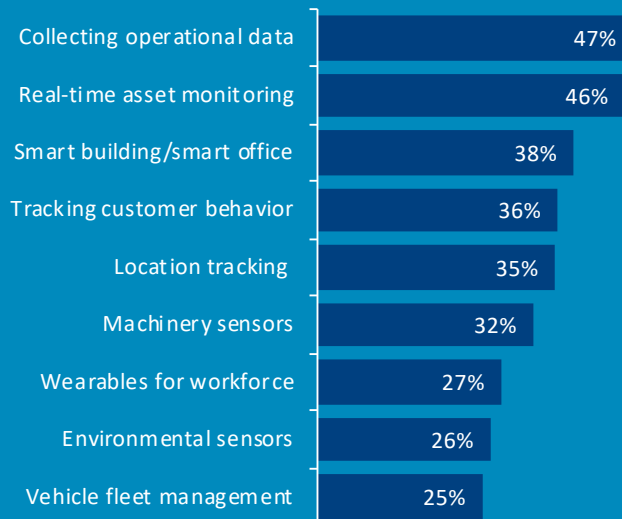
Stages of IoT adoption



Another aspect of these broad strategies is that they are not relegated solely to the IT department. As IT shifts from a tactical support organization to a strategic business partner, technology initiatives are a collaborative exercise, often being driven directly from a business unit and impacting multiple teams.

IoT clearly falls into this category. Nearly two-thirds of companies surveyed say that IoT initiatives are aimed at incorporating technology into existing business processes. This viewpoint is consistent across company size and between business/IT functions. The one exception is the executive level, where 54% see IoT as an addition to business processes and 45% see it as a standalone IT project. [FURTHER READING](#)

Types of IoT projects



Looking at the types of projects companies are pursuing, it seems clear that most fall outside of the standard IT domain. Monitoring business operations, managing the physical office environment, and tracking the behavior of customers are all activities owned by non-IT departments. Adding IoT components to these activities creates more opportunity for collaboration with the IT department, but that does not necessarily mean that they are IT projects. Those executives that connect IoT with IT may not be fully embracing a holistic view of digital transformation, where technology permeates every part of the business and new working models are needed to fully digitize operations.



MAKING THE BUSINESS CASE FOR IOT

With such a far-reaching initiative as IoT, the justification and ROI analysis will inevitably be more extensive than it is for standard IT projects. This, as with improved collaboration, is another hallmark of digital transformation. Where IT projects used to be measured primarily on the cost benefits or efficiency gains, they are now often measured by the same standards as any other corporate strategy. They must show a positive impact on overall organizational goals, many of which have never included a digital component.

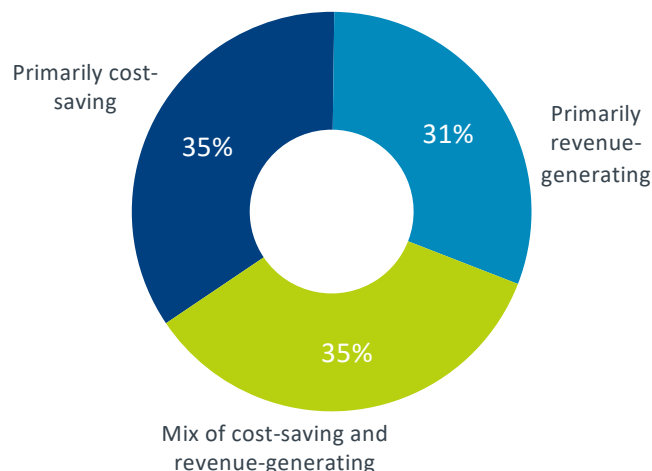
After identifying an area where IoT might be implemented, the next step is to fully understand the risks and hurdles. This step is critical at this point because so many technology projects underestimate the risks, leading to unexpected costs or problems. This is especially true when a line of business is driving the decision process. Companies are already concerned about IoT costs; 43% say that upfront costs are a major hurdle, and 34% cite ongoing costs as an issue. But if there is not a thorough assessment of other risks—such as cybersecurity (41%), interoperability (25%), or handling new data (13%)—those costs will skyrocket. [FURTHER READING](#)

On the other side of the ROI equation are the benefits companies hope to gain from IoT. Cost savings lead the list, with 43% of companies expecting that IoT will lead to a reduction in operational costs. As with other emerging technology trends, cost may ultimately prove to be a lower priority, as businesses realize that IoT's primary benefits may be improved data for decisions (38%), better asset tracking (34%) or automated business processes (32%). [FURTHER READING](#)

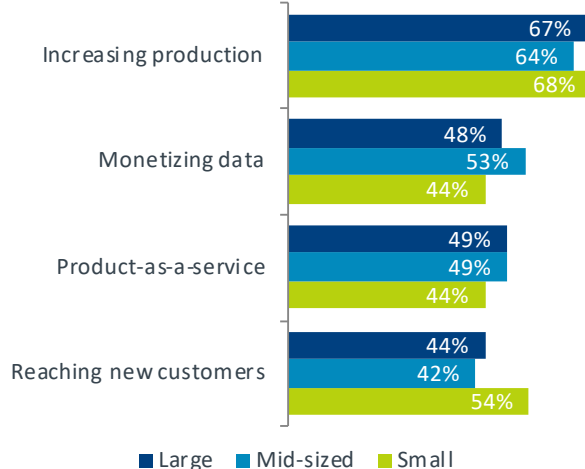
Even if current technology ROI calculations should not necessarily give the most weight to the pure financial components, that is the typical approach to IT projects. In the past, IT served more of a tactical support role and was typically viewed as a cost center. IT investments were meant to provide more IT capacity at a lower cost or greater IT capacity at the same cost. Now, as technology plays more of a strategic role, investments are evaluated more in terms of a growth mindset, looking at the overall return to the business.

Even with the focus being primarily on the finances, there is some recognition that technology is not simply a tool for cost savings. Three out of ten companies with existing IoT projects view IoT as a revenue generator, and 35% feel that there is a mix of cost savings and revenue opportunity in their IoT efforts. Large firms (500+ employees) are most likely to see IoT as potentially benefitting both cost and revenue, with 42% selecting that option. Interestingly, 33% of small firms (less than 100 employees) and medium-sized firms (100-499 employees) view IoT as primarily revenue-generating, putting those companies ahead of large firms, where only 26% take that view. The smaller firms have less operational overhead to optimize and more growth potential from trying something new, but of course they also have fewer resources to apply to the problem. This makes IoT especially interesting to solution providers, who will need to combine creativity with technical acumen when pitching IoT solutions to these clients.

View of IoT's financial impact



Uses of IoT to generate revenue



Further driving home the point that IoT is more than just a standard IT project, a majority of companies indicate that IoT funding comes from places other than the IT department. The most common source of IT funding is a new budget allocation, with 37% of companies citing this option. This demonstrates not only the importance of IoT to future strategy, but the company-wide impact that IoT tends to have. While 26% say that IoT projects are funded through discretionary IT budgets, another 19% say that the funding comes through a combination of different budget sources, once again emphasizing the holistic nature of IoT. [FURTHER READING](#)

Although the IT team may not be the primary driver from a budgeting standpoint, there is still a tremendous opportunity for IT pros and solution providers to lead the discussion on how ROI will be determined. Over half of companies in the survey (58%) say that determining ROI for IoT is "very difficult" or "moderately difficult." Again, the end goal for IoT differs from other technical projects because of the broad impact beyond cost savings. However, the technology and support needs are still the main components. This plays directly to the strengths of IT, and the ability to lead this discussion will ingrain IT further into the strategic patterns of a business.

BUILDING SKILLS FOR IOT

After a company has decided where to implement IoT and how the cost/benefit analysis works out, the next step is figuring out how to execute. Inevitably, this will lead to an evaluation of the skills that are needed for IoT success.

As with many emerging technologies, the tendency is to focus on “IoT-specific” skills. Businesses might search for an IoT Architect or an IoT Security Specialist. These positions might make sense for companies that are heavily investing in IoT strategies, but these specialized roles can mask the fact that IoT support is more likely to be a combination of existing skills that are augmented to some degree with IoT expertise.

Skills needed for IoT

	Critical skill	Needs improvement
IT security	63%	42%
Data management	61%	38%
Networking	59%	37%
Data analysis	58%	36%
Device support	55%	61%
Cloud computing	51%	36%
Artificial intelligence	36%	40%

It is no great surprise to see that IT security tops the list of skills that companies view as critical to IoT success. Merging the digital and physical worlds opens a host of potential security issues. This topic is explored further in the next section.

The next set of skills are certainly familiar to IT professionals, though there may be varying degrees of proficiency. Data management and analysis are key to unlocking the potential of IoT, but companies may need to start with basic data fundamentals if disciplined data practices are not in place. Networking and device support skills are a given in most IT departments, but companies are still looking for improvement around devices, since those are the “things” in these new systems.

The low ranking of cloud computing and artificial intelligence shows that companies may not yet appreciate how different trends complement each other. Some IoT implementations might be small, but more often they are large-scale projects. Such scale exceeds the capacity of most on-premises infrastructure, and the ongoing management and analysis requires some amount of automation. Cloud computing and AI will be necessary ingredients of any broad IoT initiative.

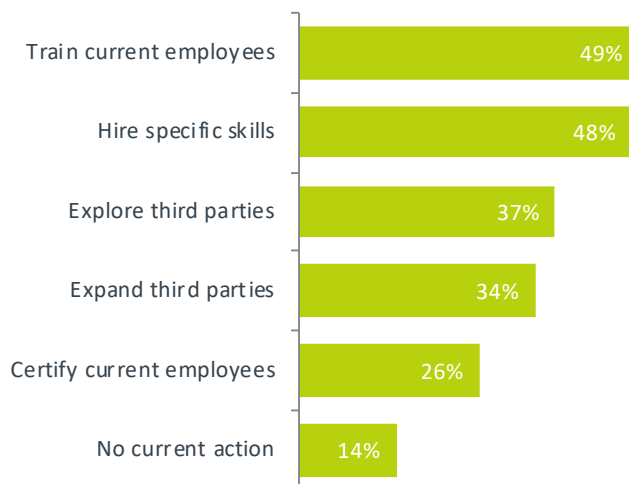
Hardware and software are not the only resources that need to be expanded for IoT. In order to fill the many different skill gaps, companies expect to utilize a wide variety of

professionals and partners.

Overall, the tendency to focus on “IoT-specific” is reflected in the types of resources that businesses expect to utilize. Three of the top four resources on the list are new IoT-specific technical staff (cited by 44% of companies), new IoT-specific vendors (38%) and new IoT-specific solution providers (38%). However, these options may be more applicable in the long-term, as robust plans are developed and these types of resources become more widely available. [FURTHER READING](#)

In the short term, companies have to work with what they have. The top option for improving IoT skills is to train current employees. This choice is understandably more popular among large and medium-sized companies, who have more resources on board that can be trained. Just over a quarter of firms in the survey plan to go beyond training and pursue certifications to validate employee expertise.

Current actions to improve skills

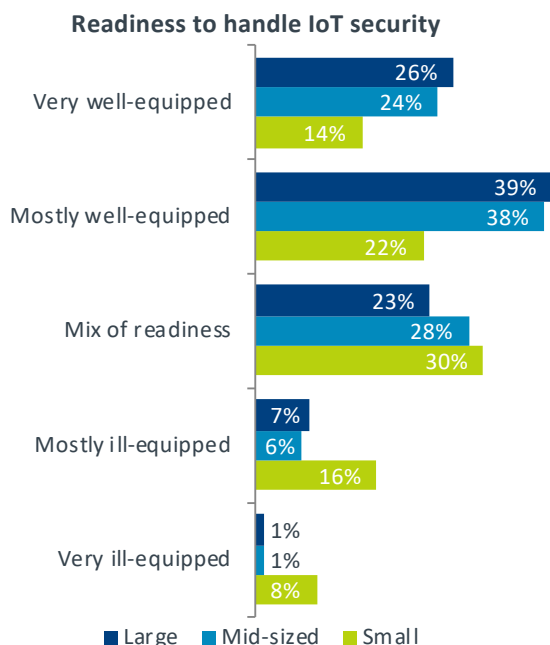


When current internal resources are scarce or hiring is challenging due to a competitive environment, third parties can provide a supplement or even take the lead on IoT activity. As with other technology trends, medium-sized firms are most likely to explore new third-party relationships or expand the partnerships they already have.

Solution providers entering the IoT space should be just as aware of the IoT ecosystem as the companies that are standing up new projects. Most solution providers will likely view IoT hardware as an adjacent space where they can provide offerings, and 68% of companies currently using a partner for IoT use them for hardware provisioning and support. The most popular way to use third parties, though, is in the area of software. The approach to software development is changing, with more companies doing custom development rather than simply purchasing packaged software. Solution providers should prioritize their own software skills, and they should also consider services around IoT systems or consulting around IoT rules and standards

FOCUSING ON IOT SECURITY

The practice of securing technology has become more difficult as new trends have entered the landscape. With cloud computing, companies had to secure resources outside their perimeter. With mobile devices, companies had to ensure that data could be secured wherever it traveled. With IoT, companies face a monumental challenge: applying digital security to processes that have never before been digitized.

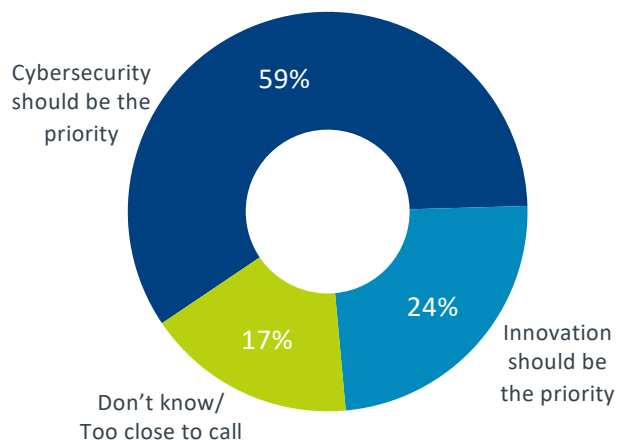


Small businesses are the least prepared for the security demands of IoT. This stems from the fact that many small firms are currently grappling with a transition to modern IT security. For many years, small businesses operated under the assumption that their digital assets were not at risk from cyberattacks. To some extent, this may have been true, but the situation has changed; all data has value, and breaches can cause more disruption than ever. The risk is magnified when physical assets and processes can be hacked.

Among the workforce, employees in business units feel the most uncertainty around IoT security. Only 9% of business staff feel very well-equipped to handle IoT security, compared to 28% of IT staff and 26% of executives. Perhaps more than any other technology, IoT is a collaborative venture. Business staff will need to educate IT about their processes and objectives, and IT staff will need to educate business units about IT practices, including security.

One of the first steps that needs to be taken for IoT security is jointly deciding on corporate attitudes towards emerging technology initiatives. With new technology, there has to be a balance between breaking new ground and ensuring a secure approach. Since some of the early fears and struggles with cloud security, companies have been shifting their mindset to proactively consider security when exploring new models. When asked specifically about IoT, most companies show a

Balancing innovation and cybersecurity



tendency toward prioritizing cybersecurity over innovation. Nearly a quarter of companies surveyed feel that innovation should be the higher priority, a mindset that may accelerate short-term adoption but introduce long-term complications.

Beyond some of the changes companies may need to make to their overall security approach, there are some IoT-specific actions that should be considered. Vendor reviews are becoming more critical when building IoT systems. A whole new wave of vendors have suddenly begun offering technology products but may not have the internal expertise to build in security. Video cameras, lighting, and vehicles are all examples of products that are quickly becoming connected and intelligent, and there is a high risk of vulnerability without a thorough consideration of the digital components and the possible attack vectors.

Another security topic that takes on greater importance with IoT is availability. Most IT professionals already build redundancy into their systems, and there are assumptions around how often the primary system might fail or how long it would take to switch over to the backup. When IoT is integrated into physical environments—especially critical infrastructure—there is a lower tolerance for failure and less flexibility in waiting for a backup to kick in. Consider an IoT system managing a building's water supply or connected to healthcare systems. The physical infrastructure that has been built for these types of situations is incredibly robust, and the digital components must be equally robust.

A final aspect of IoT security that merits careful analysis is compliance. The regulatory environment is already shifting to account for digital concerns, and this is another area where existing regulations may suddenly become the concern of IT. With regulatory compliance not being a strong suit for many firms outside highly regulated industries, the cost of compliance and the understanding of liability are major concerns. Companies will likely seek outside help in these areas, and the firms they partner with must be knowledgeable enough to take the lead in keeping their clients on the safe side.

 **FURTHER READING**

RESEARCH METHODOLOGY

This quantitative study consisted of an online survey fielded to workforce professionals during October/November 2018. A total of 506 businesses based in the United States participated in the survey, yielding an overall margin of sampling error proxy at 95% confidence of +/- 4.4 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 / Market Intelligence staff at research@comptia.org. CompTIA is a member of the market research industry's Insights Association and adheres to its internationally respected code of research standards and ethics.

ABOUT COMPTIA

The Computing Technology Industry Association (CompTIA) is a non-profit trade association serving as the voice of the information technology industry.

With approximately 2,000 member companies, 3,000 academic and training partners, 100,000-plus registered users and more than two million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications and public policy advocacy.



OTHER RESOURCES

RESEARCH

CompTIA publishes 20+ studies per year, adding to an archive of more than 100 research reports, briefs, case studies, ecosystems, and more. Much of this content includes workforce analyses, providing insights on jobs, skills, hiring practices, and professional development.

[CompTIA Research Library](#)

CERTIFICATION | LEARNING

CompTIA is the leading provider of vendor-neutral skills certifications and education of the world's IT workforce. CompTIA has four certification categories that test different knowledge standards, from entry-level to expert, in cloud computing, mobility, Linux, networking, security, help desk and technical support, servers, project management and other mission-critical technologies.

[CompTIA Certification and Resources](#)

COMMUNITIES | COUNCILS

CompTIA member communities and councils are forums for sharing best practices, collaborative problem solving, and mentoring. Discussions frequently revolve around the types of emerging trends covered in this report.

[CompTIA Communities](#)

ADVOCACY

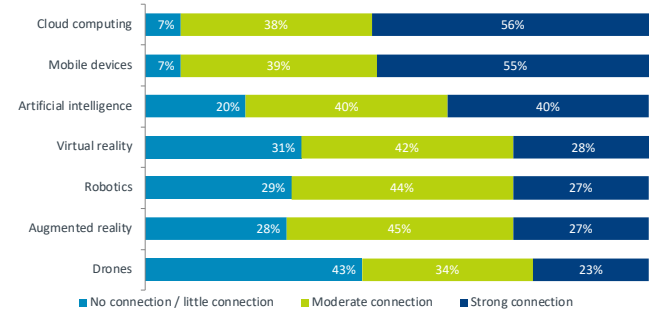
Through its public advocacy efforts, CompTIA champions member-driven business and IT priorities that impact the continuum of information technology companies – from small IT service providers and software developers to large equipment manufacturers and communications service providers. CompTIA gives eyes, ears and a voice to technology companies.

[CompTIA Advocacy](#)



APPENDIX

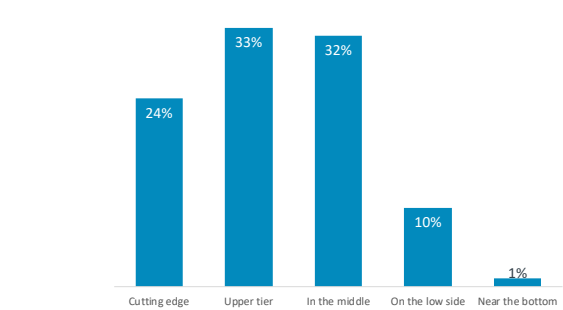
Connection between IoT and other technology



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 506 IT and business professionals in the U.S.

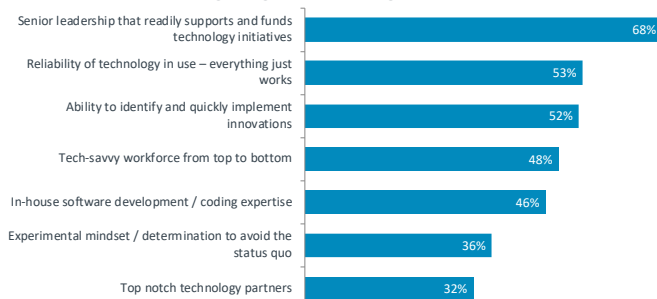
Assessment of technology utilization



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 506 IT and business professionals in the U.S.

Elements of cutting edge tech usage



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 283 IT and business professionals in the U.S.

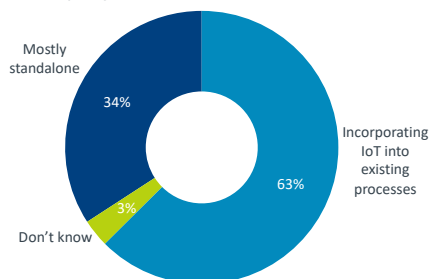
Elements of lagging tech usage



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 221 IT and business professionals in the U.S.

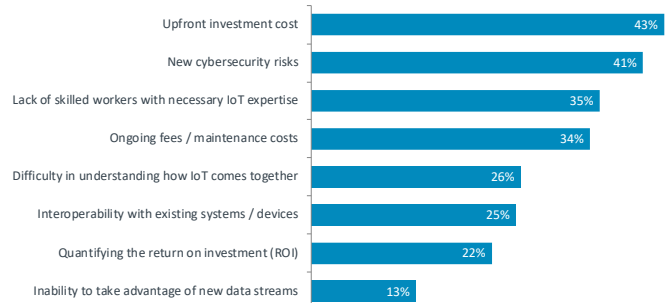
Approach to IoT projects



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 506 IT and business professionals in the U.S.

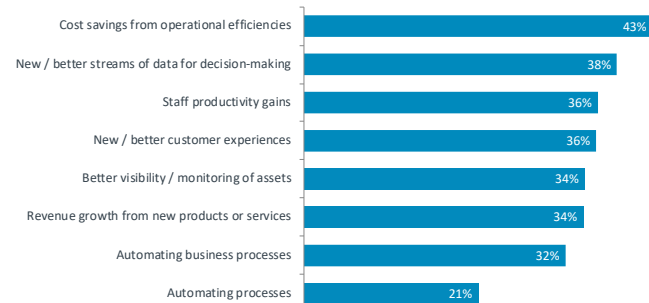
Potential Hurdles of IoT



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 283 IT and business professionals in the U.S.

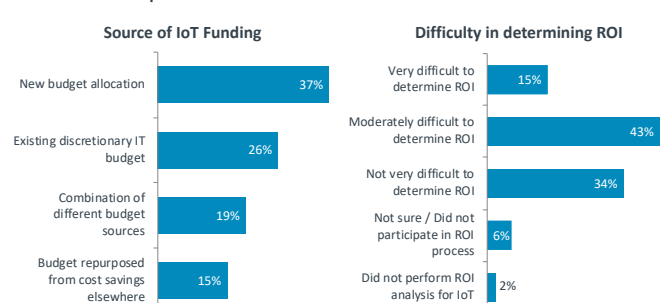
Potential Benefits of IoT



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 283 IT and business professionals in the U.S.

Financial impact of IoT

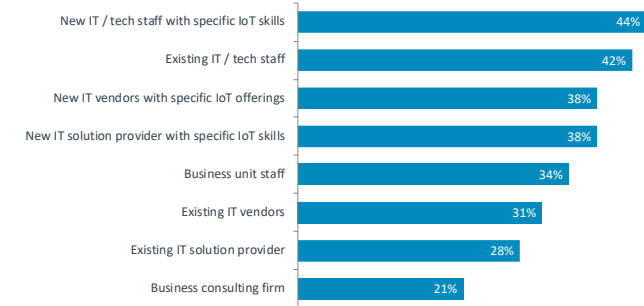


CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 248 IT and business professionals in the U.S.

APPENDIX

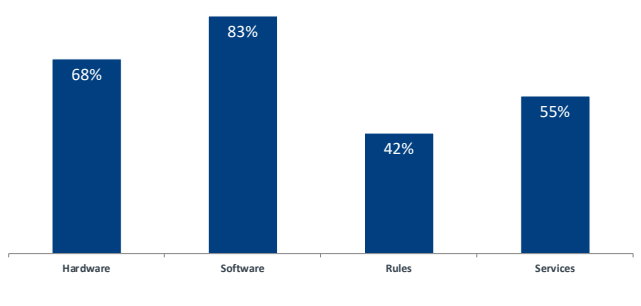
Resources involved with IoT



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 506 IT and business professionals in the U.S.

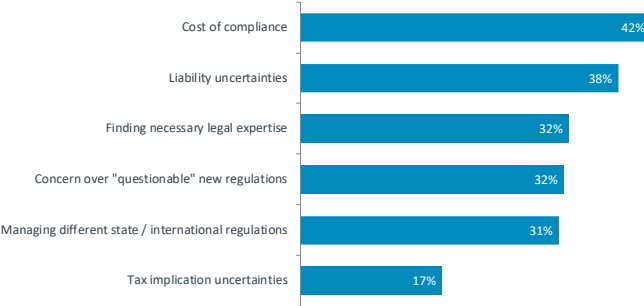
Use of solution provider in ecosystem



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 269 IT and business professionals in the U.S.

Regulatory concerns



CompTIA

Source: CompTIA's 2019 Trends in Internet of Things | n = 506 IT and business professionals in the U.S.