Leading the IoT

Gartner Insights on How to Lead in a Connected World

EDITED BY
Mark Hung, Gartner Research Vice President

Gartner®

Introduction

The Internet of Things (IoT) has rapidly become one of the most familiar — and perhaps most hyped — expressions across business and technology.

We expect to see 20 billion internet-connected things by 2020. These “things” are not general-purpose devices, such as smartphones and PCs, but dedicated-function objects, such as vending machines, jet engines, connected cars and a myriad of other examples.

The IoT will have a great impact on the economy by transforming many enterprises into digital businesses and facilitating new business models, improving efficiency and increasing employee and customer engagement. However, the ways in which enterprises can actualize any benefits will be diverse and, in some cases, painful.

The biggest barrier to the IoT is that most enterprises do not know what to do with the technology. And if they do have plans for the IoT, there is concern over who will be leading these initiatives. This need is an opportunity for CIOs to fill that IoT leadership void.

This book is intended to be a guide for CIOs and IT leaders who want to take a broader view of the IoT; it provides them with a foundation from which to start business conversations, develop their thinking and refine their approaches to accelerate time to value from IoT initiatives.

Mark Hung
Gartner Research
Vice President

Contents

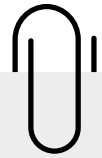
CHAPTER 1

Leverage the IoT

Commuters and pleasure travelers depend on reliable train service to get where they are going safely and with minimal delays. Train service operators want to provide that reliable service while also optimizing internal costs. Trenitalia, the main Italian service operator, leveraged the IoT in a three-year implementation plan to deliver improved reliability and compelling cost savings. With more than 1,500 train sets running more than 7,000 routes per day, Trenitalia shifted from corrective/ reactive activities and maintenance plans to a system that reflects the real conditions of each train's components.

Working together with its partner SAP, Trenitalia built a robust set of IoT use cases, associated business benefits and financial models related to optimizing train maintenance, and the team obtained buy-in from key internal stakeholders. These efforts resulted in a clearly defined three-year implementation blueprint for the Dynamic Maintenance Management System (DMMS), which partners with Italian system integrator AlmavivA for IT implementation and SAP for the data platform and analytics.

DMMS leverages onboard and ground-based sensors and diagnostics and sends that data to an on-premises private cloud for analytics in near real time. At the heart of DMMS is the transformation of maintenance from a mix of corrective/reactive activities and maintenance plans based on distance and time, to a system based on life and health indicators that reflect precisely the real physical conditions of each component of the trains. Life indicators typically measure the expected wear of components by counting relevant parameters such as cycles, time, distance and energy. Health indicators measure the actual status of component operation, such as the closing time for a door or the temperature of a cooling system.



The Internet of Things (IoT) is a network of dedicated physical objects (things) that contain embedded technology to communicate and sense or interact with their internal states or the external environment. The connecting of assets, processes and personnel enables the capture of data and events from which a company can learn behavior and usage, react with preventive action, or augment or transform business processes. The IoT is a foundational capability for the creation of a digital business.

Brake pads, for example, had always been replaced according to standard maintenance plans based on distance (kilometer) intervals. By adding a life indicator that measures the energy dissipation capability of friction braking in real time, Trenitalia now knows that route-specific factors (hills, curves and local routes with many stops), along with kilometers, have a direct bearing on brake pad life. Combined with the addition of new health measures, such as brake pressure and temperature and whether the brake is on a locomotive or a coach, Trenitalia has been able to optimize brake pad utilization and reduce maintenance activities without impacting safety or reliability.

Although Trenitalia is more than halfway through its three-year implementation plan, many other business and IT leaders are still wondering if the IoT can ever overcome the hype and fulfill its promise in organizational and societal disruption.

"Initially, leaders viewed the IoT as a silver bullet, a technology that can solve the myriad IT and business problems that their organizations faced. Very quickly, though, they recognized that without the proper framing of the problems, the IoT was essentially a solution looking for a problem," says Mark Hung, research vice president and lead analyst for IoT research. "Next, leaders started to explore the applications and use cases for which the IoT is best suited as their organizations embarked on their journeys toward digitalization. Finally, in 2017, we expect some of these 'explorers' to move to the 'reality' phase, when skunkworks projects and proofs of concept graduate to commercial or production deployment."

As IoT projects become reality for some organizations, CIOs can leverage lessons from Trenitalia's journey, aligning the IoT to desired business goals, gaining internal support for use cases and driving IoT initiatives with a roadmap and blueprint to create significant value.

Chart the path to IoT business value

The generality of the term IoT and the wide variety of delivery forms and back-end services can make it difficult to identify how to capture business value. Your first step is to move the conversation from talking about the IoT in general to talking about what it can do, or be, specific to your organization. The IoT can deliver business benefits ranging from operational improvements, such as predictive maintenance, to digital business transformation, such as selling product usage as a service.

"Initially, leaders viewed the IoT as a silver bullet, a technology that can solve the myriad IT and business problems that their organizations faced. Very quickly, though, they recognized that without the proper framing of the problems, the IoT was essentially a solution looking for a problem."

Mark Hung, Gartner Research Vice President

"Do not be shortsighted. Start with a strategic perspective by aligning use case identification with the strategic levers that drive success for your organization. Be sure to balance pragmatism (what is proven to deliver now) with vision (how the IoT can enable transformational business moments)," says Chet Geschickter, research director. "Move beyond viewing the IoT as a general technology wave by applying an industry lens to identify relevant use cases."

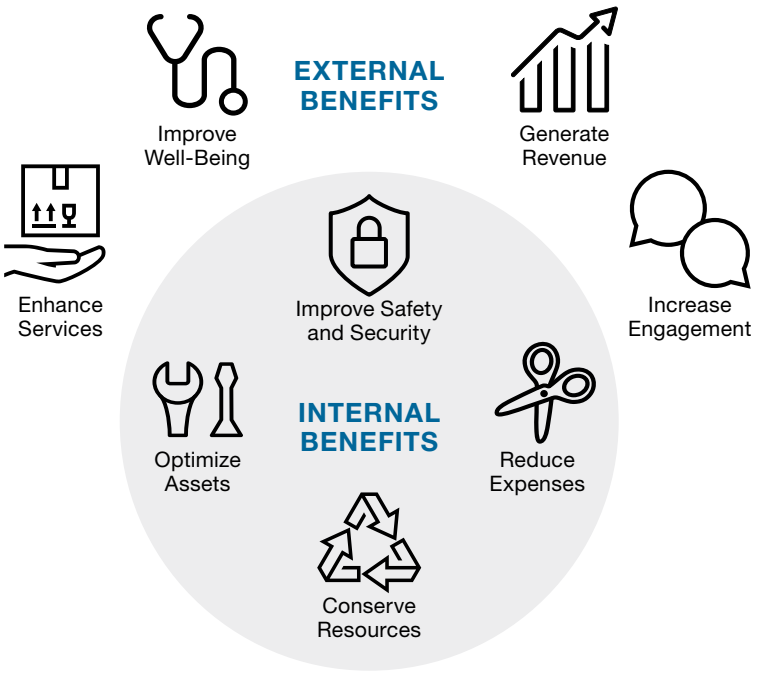
Create a basic benefits framework

The benefits from the IoT can be internally focused, such as improving your employees' safety in a hazardous production environment, or externally oriented, such as improving patient outcomes in an acute care setting. Build a basic benefits framework and organize benefits at a high level according to whether they are primarily internal or external.

"Move beyond viewing the IoT as a general technology wave by applying an industry lens to identify relevant use cases."

Chet Geschickter, Gartner Research Director

THE INTERNET OF THINGS



"Organizations should also look at the IoT in conjunction with other technologies," says Geschickter. "What happens when the IoT is combined with machine learning, advanced analytics, augmented reality or all of the above? Look at broader bundles of technologies and determine what can be done with those bundles. Combinatorial innovation is a term we use for this. What creative solutions and offerings can you build when you mix multiple transformational technologies together?"

Ensure that every IoT project has clearly identified business goals and objectives

It is essential before architecting and implementing any IoT solution that some time be spent to describe the IoT use case and value that your IoT pilot or project will deliver to your enterprise. Leaders in Trenitalia's engineering department — its CIO and other early project champions, for example — worked together with other functional leadership to gain internal support, including obtaining funding for the initiative from the company's CEO.

This step is critical, as it describes what new functionality, capabilities or differentiation your IoT project will deliver. It links these to the impact on customers, validates what basic benefits you can expect and establishes the metrics by which your IoT project's success will be measured.

Be aware that certain use cases are more likely to create compelling financial payback than others. For example, Gartner has observed that IoT use cases focused on delivering cost savings from fuel, energy and labor often have significant financial impact and shorter payback time frames. Also in this category are use cases within asset-intensive businesses or "heavy" industries. Here, industrial mechanical devices with high cost and complexity, critical asset value and remote geographic location realize IoT benefits such as remote asset monitoring and predictive maintenance that maximize asset utilization and minimize critical failure unplanned downtime.

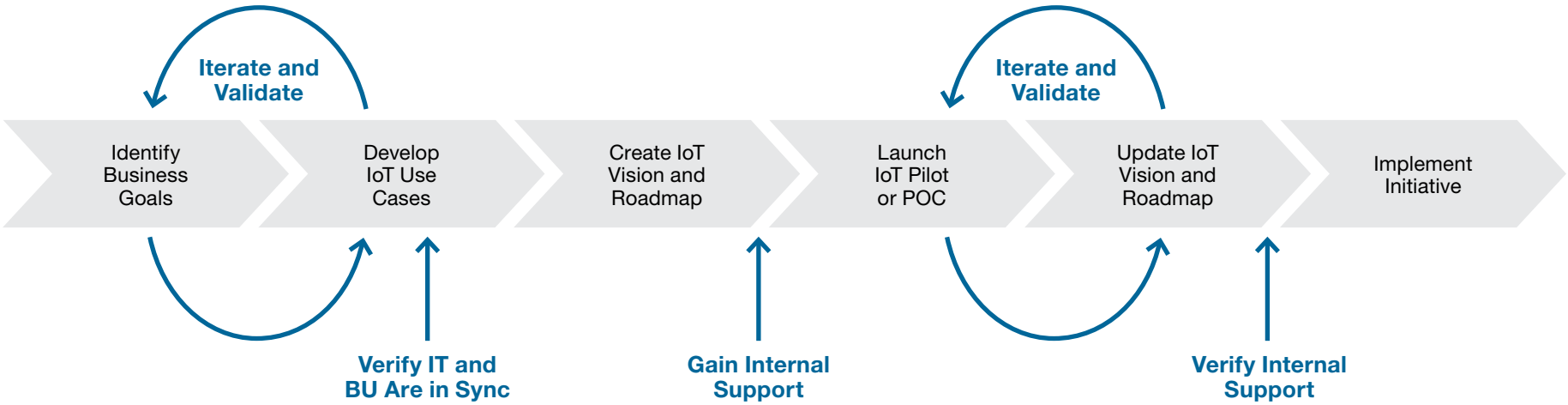
"It is critical to reassess IoT projects periodically during implementation to validate that the project will still deliver the business goals, objectives, outcomes and business value originally expected."

Nathan Nuttall, Gartner Research Director

"We often see that IoT projects are challenging for enterprises and that they take some unexpected turns as they go through the architecture and implementation process. This is due to a variety of reasons, including unexpected complexity in solution design or integration, unanticipated obstacles that need to be worked around, unforeseen performance issues in the field and solutions with higher costs than planned," says Nathan Nuttall, research director. "Most of these challenges are solvable, but they can result in IoT implementations that stray from the original plan. It is critical to reassess IoT projects periodically during implementation to validate that the project will still deliver the business goals, objectives, outcomes and business value originally expected. Otherwise, success of this IoT project and future projects in your roadmap may be jeopardized."

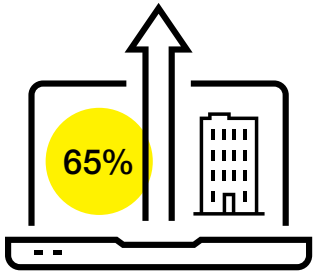
Mapping out the best practices for getting an IoT initiative off the ground, including upfront agreement and mapping of the IoT to business objectives, development of use cases and creation of a vision and roadmap, can help you stay on track to deliver on the stated business objectives as your IoT project progresses. (See figure below.)

BUSINESS PROCESS MAP FOR IoT PROJECT INITIATION



Build a blueprint

Getting your IoT project off to a good start is essential to long-term success, but the IoT is not a “one size fits all” solution. The integration of IoT technologies varies significantly among companies and industries. Implementing the right IoT solution requires an IoT architect, who must be able to employ “solution level” thinking.



By 2020, more than 65% of enterprises (up from 30% today) will adopt IoT products.

Hung says enterprises will build and adapt their IoT implementations to include a combination of five key architectural components — things, gateways, mobile devices, the cloud and the enterprise.

- **Things:** Things can be dumb or smart on their own and store most of their data on board. Things can also be self-sufficient and communicate to the internet for only centralized coordination and analysis.

Gateways: Gateways may house the application logic, store data and communicate with the internet for the things that are connected to it. Things don’t have to be as smart, because the gateway can provide these resources.

Mobile devices: Smartphones (or any mobile device) may house the application logic, store data and communicate with the internet on behalf of things that are connected to it. Things don’t have to be as smart, because the mobile device provides these abilities.

The cloud: The cloud can act as the central connection hub, power analytics and provision data storage. Things don’t have to be as smart, because the cloud will provide these resources.

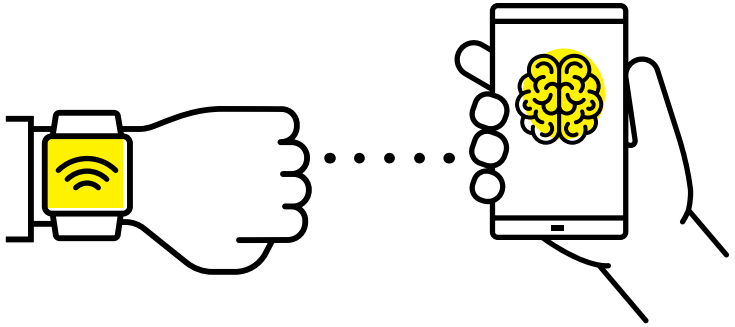
The enterprise: This architectural role is focused on keeping connected machines, application logic, and analytics and data storage on-premises — that is, behind the enterprise firewall.

"When considering the IoT, we think of machines, vehicles, buildings and consumer goods, all connected to the cloud," says Hung. "Yet, will this cloud approach be the predominant architecture for the IoT? Will we add sensors and actuators to monitor and control things, and then rely on the cloud to provide computing resources and storage? Not always."

When a fitness wristband, for example, is tethered, much of the "smartness" (the application logic) is not fully embedded in the wearable. There is some embedded application logic on the wearable, but most is in the smartphone app. At the same time, some of the applications useful to the owner are in the cloud so that the user can share fitness metrics results with friends or a healthcare provider.

Each IoT architecture will include more than one of the five functional components. CIOs must consider security, privacy, cost, ease of access, agility and performance to determine the best architecture for their specific enterprise.

The immediate challenges for most organizations, however, will be prioritizing IoT among other IT projects, such as cloud and mobile, as well as addressing underlying security concerns tied to implementing IoT.



When a fitness wristband is tethered, much of the "smartness" (the application logic) is not fully embedded in the wearable.

CHAPTER 2

Secure the IoT

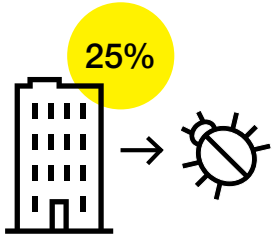
In late 2016, cybercriminals launched major distributed denial of service (DDoS) attacks, causing a disruption in internet services that affected many companies, including Amazon, PayPal, Netflix, Spotify and Twitter.

To do this, the group behind the attack exploited the security weaknesses of thousands of IoT devices, allowing them to be hijacked and turned into originators of Domain Name System (DNS) requests. Essentially, it flooded traffic to the DNS hosting provider, Dyn.

It is important to note, says Bob Gill, research vice president, that Dyn had DDoS countermeasures in place, a geographically distributed set of servers and the expertise to fight off a DDoS attack. "If an enterprise or commercial website were to be attacked with the volume and speed of this attack, it is highly unlikely they would have been able to respond as quickly or effectively," says Gill. "With over 20 billion connected things expected to be in use by 2020, you can be sure that this kind of DDoS attack is just the start."

"If an enterprise or commercial website were to be attacked with the volume and speed of this attack, it is highly unlikely they would have been able to respond as quickly or effectively."

Bob Gill, Gartner Research Vice President



By 2020, more than 25% of identified attacks in enterprises will involve the IoT, although the IoT will account for less than 10% of IT security budgets.

The IoT introduces a wide range of new security risks and challenges to the IoT devices themselves, their platforms and operating systems, their communications and even the systems to which they're connected (such as using IoT devices as an attack channel). Security technologies will be required to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications and to address new challenges such as impersonating things or denial-of-sleep attacks that drain batteries.

IoT security is often beyond the average IT leader's skill set, as it involves managing physical devices and objects rather than virtual assets. In fact, Gartner's 2016 IoT Backbone Survey showed that 32% of IT leaders cite security as a top barrier to IoT success. Understanding how to balance the promise of IoT-connected devices with potential security challenges will continue to be a megatrend in the years to come.

> **"The pace of innovation has generated requirements for millions of devices, most network (primarily wireless) connected in some capacity. Unfortunately, most of these devices have little or no protection at the software and infrastructure levels."**
>
> Earl Perkins, Gartner Research Vice President

Look beyond traditional IT security boundaries

The landscape, known as the "pervasive digital presence," changes how we approach digital security through four main differentiators from traditional IT security: scale, diversity, function and flow. Security and risk managers should consider how these differentiators are driving change and then adapt new strategies that help address the ever-shifting landscape.

"The security landscape is changing due to the scale of this digital presence," says Earl Perkins, research vice president. "The pace of innovation has generated requirements for millions of devices, most network (primarily wireless) connected in some capacity. Unfortunately, most of these devices have little or no protection at the software and infrastructure levels."

Connected devices that have been in use for many years need to safely and securely communicate with newer connected devices, particularly in the world of industrial automation and control systems. For example, with the diversity of devices and environments in which they operate, there is no single standard for device-to-device authentication or how devices can securely link to cloud services.

Another differentiator in IoT security is how typical IoT devices function. Many devices are constructed to be "fit for purpose," in that they are created to perform specific functions that may require only a few operations, such as a sensor detecting five characteristics of an environment or an actuator performing to commands. The rise of the IoT creates a varied and different approach to device function — some devices may be built to only deliver information by the second, while others act as a static storing place for information until something is triggered.

Finally, security and risk decision makers must look at data flow in IoT networks to understand how, when and where to secure data. Data in IoT networks tends to be constantly changing, even if it's stored. When making key decisions to protect data via encryption, network segmentation or even monitoring and detection, data flow remains a key differentiating characteristic that may require new approaches in digital security.

The rise of hardware security

The IoT creates new security challenges for enterprises in both scope and scale. Embedded hardware security provides IoT project leaders with a new set of tools to address these new security requirements. However, traditional digital security tenets must be re-examined in the era of IoT:

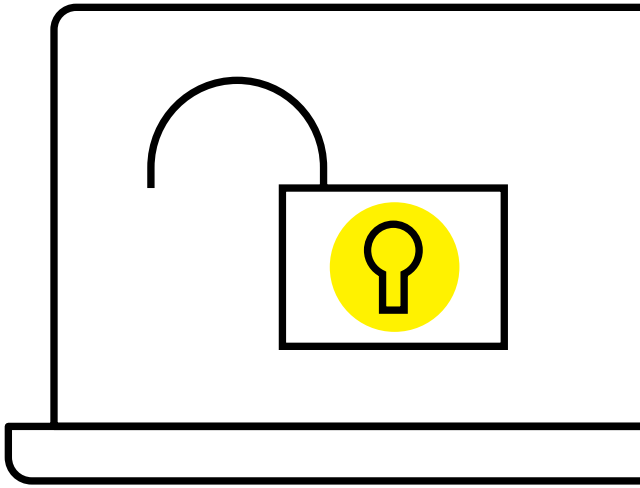
Device identity: The IoT requires strong device identity and Root of Trust at its foundation. This remains a weakness on the PC platform. Hardware-based security, where appropriate, is a key ingredient for enabling this functionality.

Secure network scale: For many IoT deployments, the number of IoT endpoints will dwarf those in traditional IT projects. Securely managing the network connections and data across these devices requires a scalable solution. Today, public key infrastructure (PKI) is often used to enable trust between systems based on digital certificates. PKI has been proven to scale; however, the device and environmental characteristics of the IoT create a challenge for the secure issuance and processing of certificates. Coupling PKI with a strong device identity is a solution to this problem.

Data security and physical security: Building security into the data itself, whether it is in transit (data communication) or at rest (data storage), is valuable in the IoT, given the lack of physical security that resists tampering for most devices. Therefore, tamper-resistant physical security — which can be addressed with hardware security — becomes critical. Key control data and sensor data are now accessible, which can also be addressed with hardware security.

"To address these issues, security mechanisms that leverage hardware-based implementations are gaining momentum. Hardware-based implementations, for some types of applications, can offer additional security features that mitigate against a number of attacks that software-based solutions cannot," says Hung.

In some industries, mandates for hardware security are already in place. For example, in the financial sector, credit cards are required to use chip-based authentication to meet the EMV standard. Specifically, one of the key drivers behind EMV being hardware based is to provide anti-tampering mechanisms to prevent card cloning. Other sectors, such as healthcare and industrial, are likely to follow. It is not hard to imagine that hardware security will one day become as integral a part of an IoT device as the GPU or math co-processor is to the PC.



CHAPTER 3

Staff the IoT

You, the CIO, get an urgent message from your CEO. You stare at the message, thrilled and nervous.

Dear CIO:

I have selected you as the IoT leader for our company. The first thing I'd like you to do is determine the key steps in leading our IoT efforts and draft your dream team. Then come back to me in a week so we can discuss how the team will achieve the company's IoT objectives and satisfy the board's growing interest in using digital business and the IoT for competitive advantage.

Good luck,
Your CEO

Where do you start? What capabilities will you need? How do you recruit or develop the talent needed to enable the IoT in your organization?

The CIO of Everything

As the IoT becomes more prevalent, the CIO — often the most "techie" person at the company — will be asked to step up and lead the effort. In a recent Gartner survey, almost one-third of responding organizations expected that the CIO would be leading their IoT activities.

"Don't underestimate the unknown factors that will emerge as the IoT expands and the enterprise's IoT participation grows," says Jenny Beresford, research director. "The IoT will expand rapidly and extensively, continually surfacing novel and unforeseen opportunities and threats."

This calls for a new type of CIO, a "CIO of Everything," who can radically adapt their vision, decision making and capabilities to orchestrate an IoT world.

By 2020, more than 10% of new IoT products from traditional industries will be headed by the CIO.

"Enterprises will approach the IoT from different angles — perhaps as consumers of fresh lakes of data, or as passive contributors of data points into the IoT, or as active IoT ecosystem leaders bringing new product and intelligence to market," says Beresford. "Whatever the point of entry for a cultivated enterprise IoT, the ability to act with speed, imagination and confidence is a quality required of the CIO of Everything. They will be expected to own, respond to and resolve the waves of new and unanticipated demands, considerations and issues that the IoT will generate on a daily basis."

"Whatever the point of entry for a cultivated enterprise IoT, the ability to act with speed, imagination and confidence is a quality required of the CIO of Everything."

Jenny Beresford, Gartner Research Director

CHALLENGES AND STRATEGIES FOR THE CIO OF EVERYTHING

- Take the IoT lead in the C-suite
- Improve strategic thinking and risk appetite
- Practice agile IoT product development

- Develop the IoT strategy and roadmap
- Map and monitor the IoT ecosystem
- Build dedicated IoT capability

- Reduce limitations and mitigate risks
- Practice rapid decision making
- Build trust and teamwork

Build a dedicated IoT team for the enterprise

The CIO of Everything will need a dedicated IoT team to design and grow the enterprise's IoT participation from Day 1. This team needs to be skilled in designing, mapping, reading, growing and maintaining the enterprise's IoT internal domains and external products.

"The CIO will need a curious, entrepreneurial and strategic-thinking IoT-focused team able to work with abstraction and unprecedented levels of complexity, and to anticipate opportunities and threats quickly as industry and market conditions and technologies change," says Beresford. "Brainstorm needs with IT leaders and forward-thinking business leaders and product owners to develop a profile of the talent, skills and competencies needed to form and develop this new pivotal team."

"As with any emerging technology, the recipe for success involves a mix of technical knowledge, business acumen and delivery skills."

Erik T. Heidt, Gartner Research Vice President

The emergence of the IoT architect

On the IoT team, the IoT architect will emerge as the central linchpin role for planning, executing and governing IoT.

Not everyone who will provide the needed IoT skills will be an IoT architect, but IoT delivery teams will need individuals in this role. The IoT architect is responsible for:

1. Engaging and collaborating with stakeholders to establish an IoT vision and define clear business objectives
2. Designing an edge-to-enterprise IoT architecture
3. Establishing processes for constructing and operating IoT solutions
4. Working with the organization's architecture and technical teams to deliver value

"These individuals will be hard to find," says Erik T. Heidt, research vice president. "As with any emerging technology, the recipe for success involves a mix of technical knowledge, business acumen and delivery skills. The possession of superior capabilities in any one of these three areas will distinguish many technical professionals from their peers. Those having such capabilities in two or more of these areas will be in extremely high demand. The good news is that organizations can use existing digital business efforts to train up candidates."

Organizations need to understand the importance of the IoT architecture itself, as well as the IoT architect role. Waiting for business demand for IoT to raise architectural questions and issues down the road will put technical professionals in a reactive position.

The role of the enterprise architect

IoT architecture and technologies have the potential to transform industries and the way we live and work. “Enterprise architecture (EA) and technology innovation leaders are in a great position to lead their organizations’ response to the opportunities and threats of IoT technologies,” says Mike J. Walker, research director. “They are also well placed to evaluate the impact of these technologies on business models and to assess the technology risks.”

Gartner has identified five ways enterprise architects can address top IoT challenges:

1. Adopt ideation-based approaches to exploit the IoT’s potential:
Using an ideation-based process, EA and technology innovation leaders can understand the characteristics of a specific IoT technology and identify the technology’s business opportunity. Through this ideation, they can provide business unit and IT leaders with more than just a list of “cool” technology ideas. For example, they could provide a broad understanding of the business impacts of IoT technologies, based on the technologies’ characteristics, the information they expose and how they will be used.

2. Create business scenarios for the use of IoT technologies:
Building on ideation and understanding IoT technology isn’t enough. Business scenarios are a forward-looking way for organizations to describe how IoT technologies can introduce new value streams. They can also enhance existing ones by combining innovative technologies with possible future business models. EA and technology innovation leaders should partner with business leaders and experts to define the opportunity or challenges in business scenarios.

3. Manage risks by devising IoT information architecture:
IoT technologies break down the traditional view of security because organizations must shift from an information security approach to a risk management approach when assessing which opportunities are viable. Once organizations have identified the business opportunities of IoT technologies by using business scenarios, they can identify the context needed to understand the effects of the information in IoT solutions.

4. Partner with other roles to develop an interoperability strategy:
Fixing business outcomes, devising business scenarios and defining business information give IoT initiatives a solid foundation for understanding how to approach interoperability. Although EA and technology innovation leaders don’t own the interoperability strategy, they should partner with and guide integration architects and other related technology roles to develop an interoperability strategy.

5. Focus on providing IoT experiences users want:
Organizations will only gain competitive advantage from IoT technologies if they make them simple, useful and intuitive for users. The technologies alone won’t gain mainstream adoption if they don’t address a specific purpose and enhance the user experience. EA and technology innovation leaders must understand how users want to use IoT technologies — and in what environments — while also understanding users’ cultures. This is where personas come into play. Personas can be used to humanize the target audience of a solution with a view to provide a better user experience.

> "Enterprise architecture (EA) and technology innovation leaders are in a great position to lead their organizations' response to the opportunities and threats of IoT technologies."
>
> Mike J. Walker, Gartner Research Director

In light of digital business, the IoT already has a significant impact if harnessed and exploited effectively. It represents the basis of providing competitive advantage. Organizations that are not focused on the IoT and its impact must consider using EA and IoT architecture as one of the more important strategic elements contributing to business success. Because the IoT is a building block to digital business, EA and IoT architects will be critical to enable it to reach its full potential.

Demand for data scientists

IoT systems often involve huge amounts of data from a wide variety of sources, including sensors, situational data such as a "thing" location, forecast data such as the weather, contextual data (identity of the user) and operational data to manage the IoT system.

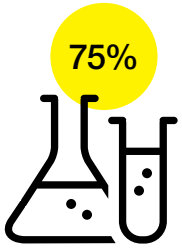
To create business value, this data must be converted into decisions and actions. In general, this implies a hierarchy of analytic sophistication, with the most valuable decisions and actions demanding the most sophisticated analytic and simulation tools. Some of the most sophisticated IoT solutions go beyond analytics to exploit the idea of a "digital twin," which uses a software model of a "thing" or system that can be used to understand and even predict its behavior.

Data science and digital twins aren't limited to supporting operational decisions; they also facilitate innovation by providing insights into how products and services are being used and can be improved. For example, analyzing how a thermostat is used might suggest energy optimizations, or knowing how a car is driven might unearth new features to reduce accidents.

Effective exploitation of IoT will therefore demand data scientists and simulation experts to analyze data and create digital twin models. Such staff must understand not only data science principles but also some of the tools that are specific to IoT situations — for example, stream-processing platforms and gateway analytics.

Additionally, in industrial IoT scenarios, much of the insight on how assets perform is also understood by plant managers, equipment technicians and others whose knowledge is valuable as input into IoT analysis. However, such skills are in demand, data scientists' salaries are high and organizations may not be able to obtain the staff they require.

Although universities are scaling up education in data science, it will likely take five or more years before the supply of skills improves substantially. The growing number of organizations using the IoT or refining early projects to use IoT in more sophisticated ways is likely to keep demand high for several years. CIOs and IoT architects should look at retraining to partly satisfy the demand for skills in the short term. However, because staff with the necessary skills will be scarce or expensive, organizations will seek ways to use them more effectively or will find alternatives to human involvement, perhaps using machine learning rather than human data analysis.



Through 2020, a lack of data science specialists will inhibit 75% of organizations from achieving the full potential of IoT.

CHAPTER 4

Exploit the IoT

When 45,000 cans of Budweiser beer arrived in a Colorado warehouse after traveling over 120 miles down a highway in a self-driving truck, it became the first revenue-generating load to be transported by an autonomous vehicle.

The truckload of beer was shipped from Fort Collins to Colorado Springs by Otto, the self-driving truck subsidiary of Uber, with the driver monitoring the two-hour journey from the truck's sleeper berth.

Is this the future of road freight? According to Greg Aimi, research director, some of the earliest applications of autonomous technology for self-driving trucks are likely to be on the long hauls of highways, as today's technology is best suited to the relatively high predictability of the route, rather than navigating busy urban streets where more rules, route variations and complicated maneuvers are required.

"It's still the early days for driverless trucks, and Gartner predicts that by 2021, less than 1% of long-haul, over-the-road freight will be carried by autonomous trucks," says Aimi. "However, when you consider that the heavy- and medium-duty commercial truck sector — which carries the majority of over-the-road freight in the U.S. — comprises 3.6 million vehicles, this still means that within five years there could be up to 36,000 autonomous trucks traveling U.S. highways."

"Some of the earliest applications of autonomous technology for self-driving trucks are likely to be on the long hauls of highways."

Greg Aimi, Gartner Research Director

"Until clear leaders and standards begin to emerge … we will continue to see different alliances forming around the autonomous vehicle initiatives."

Michael Ramsey, Gartner Research Director

Driverless or autonomous vehicles for many applications already exist, but are not yet commercially available for over-the-road use everywhere. Investments, including $4 billion from the U.S. government, are pouring into the new technologies as first movers jockey for leadership positions.

However, Michael Ramsey, research director, says the biggest hurdle to autonomous vehicles becoming mainstream will likely be regulatory. Governments will need to feel comfortable with the rules put in place before these cars and trucks are released to the general public.

The current state of autonomous vehicle development is still a bit fragmented — automobile manufacturers, large technology providers, chip companies and lesser-known tech innovators are all vying for a seat at the table. "The critical capabilities for automated driving cluster around sensing technologies, 3D mapping and data analytics, and algorithms for computer vision, localization and path planning," says Ramsey. "Until clear leaders and standards begin to emerge in each of these areas, we will continue to see different alliances forming around the autonomous vehicle initiatives of leading car companies."

The connected home

In the connected home, a garden-watering system might monitor and irrigate plants and be connected to and controlled by a smartphone app. In a more complex system, the watering system would be connected to the water supply utility and use intelligent cloud services to combine weather forecasts and pricing to minimize costs. In times of drought, the system might prioritize using limited water supplies for more valuable plants.

“The technologies and commercial effects of the connected home could have a wide-reaching impact on the role of CIOs, depending on the company and products,” says Nick Jones, vice president and distinguished analyst. “However, the connected home also represents an opportunity for CIOs to be involved in the implementation and operation of new products and strategies. CIOs could be directly or indirectly impacted by the smart home, depending on whether the company is creating the connected products and services or determining how other companies’ products will affect security.”

Currently, homeowners can get a rudimentary connected home for less than $100, which would include a smart plug and an app. However, they need to spend several hundred dollars to get a truly connected home, including a virtual personal assistant- (VPA-) enabled wireless speaker, a smart lighting kit, door and window sensors, smart locks and home-monitoring cameras.

They also need to be aware that the more connected things there are, the more chance there is that they will have to use multiple apps to control and monitor their home. “Consumers are increasingly looking for one app for one integrated smart ecosystem,” says Jessica Ekholm, research vice president. “As a result, for connected-home products to achieve mass-market adoption, continued efforts are needed to integrate providers and apps. The industry is moving toward further integration with the API ecosystem, and there are a growing number of connected home cloud hubs that help users enjoy a more seamless experience at home.”

“Consumers are increasingly looking for one app for one integrated smart ecosystem.”

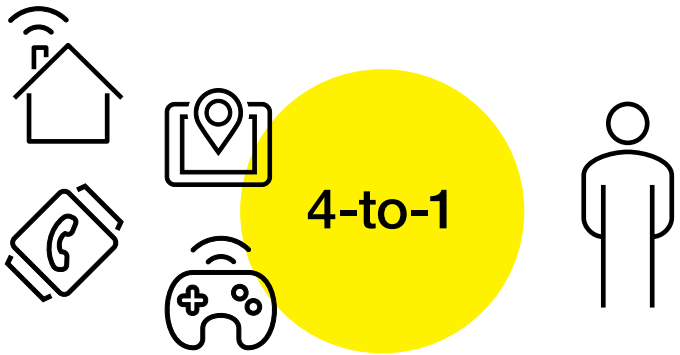
Jessica Ekholm, Gartner Research Vice President

Prepare to do business with things as they become customers

The customer experience takes a new twist in the IoT era, with many customers not actually being human. What if your customer's electric vehicle found the nearest charging station, reserved a spot and then paid your company for it? Or your customer's dishwasher told you, the manufacturer, when it was ready for service and scheduled the service call on the customer's behalf?

Things becoming customers will fundamentally change the vendor/customer relationship in many industries. The devices allow for a new relationship, one that bypasses the distributor and retailer intermediaries that currently intercede in the vendor-to-consumer relationship. Because their devices do much of the decision making for them, consumers will be able to bypass the retailing and service/repair channels that currently exist.

"This may seem far-fetched, but it's not, and organizations that fail to build for such eventualities are at risk of obsolescence," says Don Scheibenreif, vice president and distinguished analyst. "We know that today, internet-connected things can already identify themselves and even locate themselves. Machine-to-machine communication means they will have the ability to communicate — with each other, with customers and with businesses. Things will make lives easier, both at work and outside of work, by handling routine tasks, and it's not a stretch to see how they will move from simple ordering to negotiating."



By 2020, Gartner estimates internet-connected things will outnumber humans 4-to-1, creating new dynamics for marketing, sales and customer service.

"The IoT will do more for us today and in the future than we have yet to imagine," says Scheibenreif. "Things will become your customers or will act on behalf of customers, as their agents. It is a future both intriguing and scary. However, whether your organization is excited or spooked at the prospect of intelligent things as customers, it's important to remember that humans will be able to set the parameters for most things. Human customers will programmatically tell things what to do, and organizations will have the ability to turn off the things."

"The IoT will do more for us today and in the future than we have yet to imagine. Things will become your customers or will act on behalf of customers, as their agents."

Don Scheibenreif, Gartner Research Vice President and Distinguished Analyst

Additional Research

Chapter 1: Leverage the IoT

CLIENT RESEARCH

IoT's Challenges and Opportunities in 2017: A Gartner Trend Insight Report
Mark Hung, April 2017

Trenitalia Drives Cost Savings Using IoT on Train Operations
Nathan Nuttall, December 2016

SMARTER WITH GARTNER ARTICLES

The IoT Effect: Opportunities and Challenges
Smarter With Gartner, March 2017

Chart the Path to IoT Business Value
Smarter With Gartner, February 2017

How CIOs Should Launch an IoT Product
Smarter With Gartner, September 2016

Build a Blueprint for the Internet of Things
Smarter With Gartner, May 2016

Chapter 2: Secure the IoT

CLIENT RESEARCH

Forecast Alert: Internet of Things — Endpoints and Associated Services, Worldwide, 2016
Peter Middleton, January 2017

Survey Analysis: 2016 Internet of Things Backbone Survey
Nathan Nuttall, Eric Goodness, Mark Hung, Chet Geschickter, January 2017

Hardware Security and Its Impact on IoT Projects
Mark Hung, Anmol Singh, David Anthony Mahdi, October 2016

SMARTER WITH GARTNER ARTICLES

Navigating the Security Landscape in the IoT Era
Smarter With Gartner, December 2016

The IoT Effect: Opportunities and Challenges
Smarter With Gartner, March 2017

GARTNER BLOG NETWORK

The Internet just got punched in the face
Andrew Lerner, Guest blog from Bob Gill, October 2016

Chapter 3: Staff the IoT

CLIENT RESEARCH

2017 Planning Guide for the Internet of Things
Erik T. Heidt, October 2016

Predicts 2017: IoT Proliferation Will Drive Investment in New Approaches to Implementation
Benoit J. Lheureux, Earl Perkins, Denise Rueb, Nick Jones, Yefim V. Natis, Alfonso Velosa, January 2017

Toolkit: An Enterprise Architect's Guide to Ideation
Mike J. Walker, March 2017

SMARTER WITH GARTNER ARTICLES

Be the CIO of Everything
Smarter With Gartner, April 2017

How CIOs Should Launch an IoT Project
Smarter With Gartner, September 2016

Use Enterprise Architecture to Unlock the Transformational Potential of IoT
Smarter With Gartner, January 2017

Chapter 4: Exploit the IoT

CLIENT RESEARCH

Top 10 IoT Technologies for 2017 and 2018
Nick Jones, January 2016

Hype Cycle for the Internet of Things, 2016
Alfonso Velosa, W. Roy Schulte, Benoit J. Lheureux, July 2016

SMARTER WITH GARTNER ARTICLES

Autonomous Trucks Arriving at a Warehouse Near You
Smarter With Gartner, December 2016

The Road to Connected Autonomous Cars
Smarter With Gartner, December 2016

Why CIOs Should Care About the Connected Home
Smarter With Gartner, August 2016

Control the Connected Home With Virtual Personal Assistants
Smarter With Gartner, February 2017

When Things Become Customers
Smarter With Gartner, July 2015

7 Technologies Underpin the Hype Cycle for the Internet of Things, 2016
Smarter With Gartner, November 2016

Gartner®