2018 Planning Guide for the Internet of Things

Published: 29 September 2017 **ID:** G00331852

Analyst(s): Erik T. Heidt

In 2018, IT organizations will continue to receive pressure from business units and operational technology groups to support a variety of IoT-enabled solutions. Technical professionals must address stakeholder concerns about their ability to deliver, operate and maintain IoT systems.

Key Findings

- Stakeholders' and sponsors' risk concerns span a wide range of topics. The information security of Internet of Things (IoT) systems tops the list, but concerns about delivery capability, service quality, reliability and safety must also be addressed.
- IoT design patterns are maturing. 2018 will see clear models for IoT edge computing and hybrid platforms emerge, separating hype from practical application.
- The development of an IoT technical strategy is central to addressing stakeholder and sponsor concerns regarding readiness. Organizations should not delay identifying an IoT architect or developing a target IoT architecture.

Recommendations

Technical professionals responsible for the development, implementation and operation of IoT:

- Use lightweight, early engagement activities to demonstrate IT's commitment and capacity to delivery IoT. The most important early IoT activity is documenting specific business opportunities.
- Develop a target IoT architecture now. A "straw man" architecture is an effective tool for driving engagement, planning and knowledge sharing among OT, IT and stakeholder groups. There will be no perfect architecture — do not allow the drive for perfection to be the enemy of progress.
- Familiarize yourself with the IoT design patterns that are emerging in 2018, and determine if they are relevant to your organization's business and technical problems.
- Define processes to address the onboarding of third-party and outside IoT solutions. Ad hoc requests often create disruptive, unplanned work, but failure to address these needs raises concerns about IT's ability to execute on IoT in general.

Table of Contents

List of Figures

Internet of Things Trends

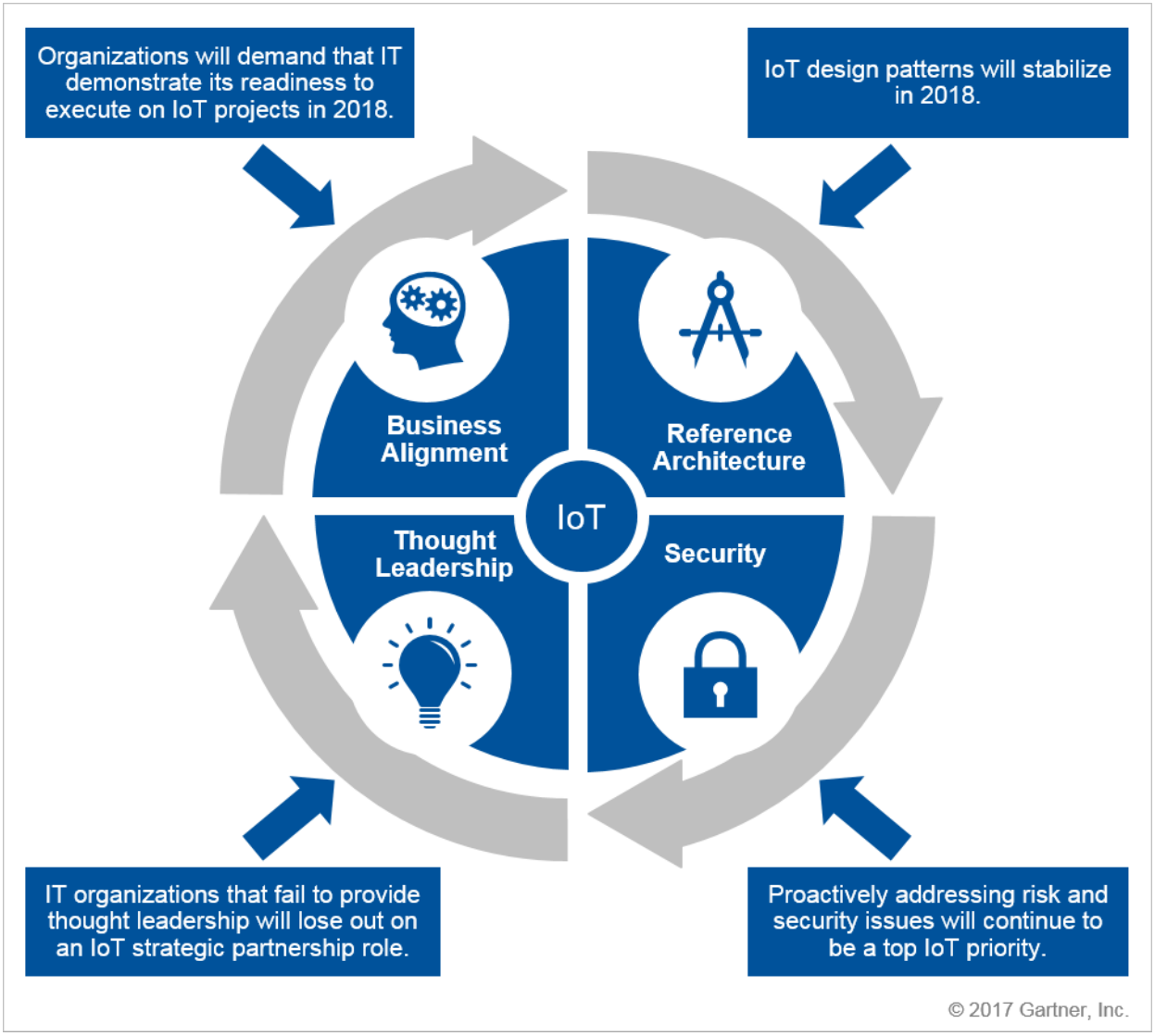
Many organizations have concerns about how prepared the IT organization is to execute on IoT. Such concerns pose significant barriers to adoption, and must be overcome for IT to assume an IoT thought leadership role. Some of these concerns originate from stakeholder anxiety regarding the changes IoT brings to current operations. Some of the concerns originate from skills gaps. In many cases, a third source of concerns stems from criticisms levied during intraorganization posturing over the "ownership of IoT." All of these concerns can be overcome through engagement, architecture and a plan that proactively addresses these issues.

Large quantities of devices and equipment are being IoT-enabled by their manufacturers. This is causing an influx of new edge technologies, which is disrupting network operations and many governance functions. This "organic IoT" trend results from enabling existing capabilities. Some business groups are exploiting this technology by forging ahead and launching IoT initiatives without the IT organization's participation, in an attempt to reap quick business benefits. Such "shadow IoT" initiatives often fail to meet nonfunctional requirements, are duplicative or can't be maintained. As such efforts proliferate, the result will be lost productivity, lost information and lost opportunities, while the IT organization watches from the sidelines. IT must provide thought leadership to avoid this chaos.

This Planning Guide identifies key trends and planning considerations that technical professionals must understand to help their IT organizations demonstrate IoT competence and thought leadership (see Figure 1). The guidance in this document focuses on the following trends:

- **IT organizations that fail to provide thought leadership will lose out on an IoT strategic partnership role.** Stakeholders will find strategic partners with which to execute IoT. In 2018, IT will either step up and demonstrate thought leadership or lose out on this critical leadership (and value) opportunity. To avoid this fate, IT must demonstrate its value as a strategic IoT technology partner, while simultaneously addressing current unplanned IoT work.
- **Organizations will demand that IT demonstrate its readiness to execute on IoT projects in 2018.** Technical strategy is the key tool that technical professionals will use to address questions about current and future capability. In addition, IT organizations will need to treat business needs as their "true north," and should leverage an IoT reference model. Failure to align the organization's IoT efforts to a target architecture results in technology sprawl, redundancies and inefficiencies that drive up cost, reduce quality and slow innovation.
- **IoT design patterns will stabilize in 2018.** As organizations deploy IoT to support more complex and demanding use cases, new design patterns are emerging. During 2018, the edge-computing and unifying-platform patterns will become implementation styles that all major suppliers will support and reference.
- **Proactively addressing risk and security will continue to be a top IoT priority.** Risk and security issues continue to be a major obstacle to IoT adoption. Addressing these areas will be a key planning focus in 2018.

Figure 1. IoT Planning Trends



Source: Gartner (September 2017)

IT Organizations That Fail to Provide Thought Leadership Will Lose Out on an IoT Strategic Partnership Role

Technology is the new business medium. As a result, IT organizations that are reactive to emerging technologies such as IoT consistently demonstrate less business value than organizations where IT acts as business partner that is directly involved in the identification and execution of strategic business innovations.

A recent cloud-related IT trend will likely play out again for IoT. IT's reluctance to embrace SaaS led many organizations to take a "shadow IT" approach to SaaS adoption, bypassing IT. Many IT organizations weren't informed of SaaS or other cloud service decisions until after they were made

by the business, relegating IT to a "cloud catcher" role. These IT groups were not acting as partners or enablers for the business. When it comes to IoT, IT must engage with the organization and assume a thought leadership role. Otherwise, IoT will become a repeat of SaaS and other shadow IT initiatives, and IT will miss out on yet another opportunity to create value and improve outcomes.

As IoT continues to emerge, it will present this challenge: IT organizations will risk becoming "IoT catchers" rather than strategic partners in IoT. Several factors increase this risk for IoT initiatives:

- **Operational technology (OT) as IoT owner:** Many organizations find it difficult to create a collaborative relationship between OT and IT. "Turf wars" between these groups are counterproductive, and will delay the business value IoT has to offer.
- **Lack of confidence in execution ability:** Organizations are delaying and deferring IoT projects due to concerns about their readiness and ability to execute. IoT solutions are complex and modify critical services. Stakeholders must weigh the risk of IoT project failure, and this is causing many organization to either forgo certain projects or avoid IoT altogether.
- **Failure to address organic IoT, leading to a perception of overall IoT failure:** Many IT departments are struggling with a flood of organic IoT growth. IT departments that don't proactively address this issue will have a harder time convincing business partners and OT groups that they are a credible IoT partner.

The crux of the challenge for IT organizations is to simultaneously demonstrate IT's value as a strategic IoT technology partner while addressing current unplanned IoT work.

Planning Considerations

Business demand for IoT is increasing, but adoption is lagging. Many organizations do not feel prepared to move forward with IoT. To position themselves as the IoT partner of choice, IT organizations must inspire confidence and demonstrate their capabilities. Key planning steps to address this challenge include:

- Hiring and empowering an IoT architect
- Sponsoring IoT workshops and labs
- Proactively addressing organic IoT

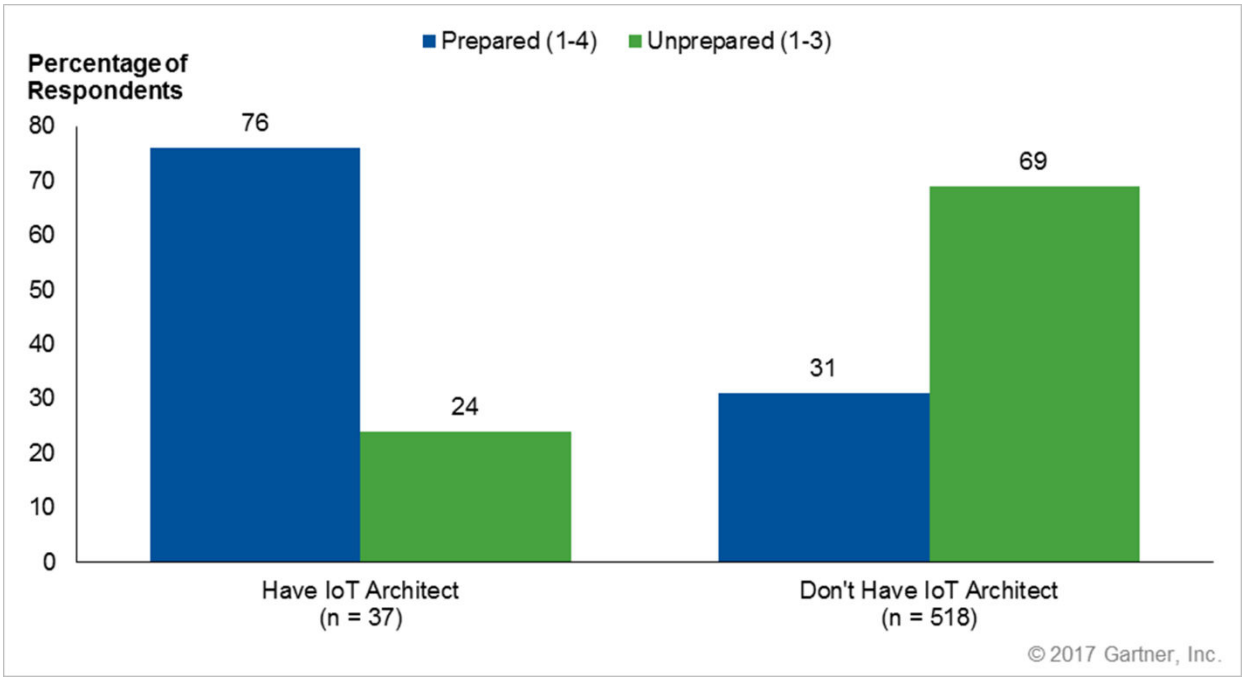
Hire and Empower an IoT Architect

Want to dramatically improve your organization's ability to execute IoT, as well as stakeholder perceptions of that ability? Recruit and empower an IoT architect. Technology and solution architecture is a well-established approach for improving the effectiveness, efficiency and quality of a wide range of technology functions — and IoT is no exception.

Reaping business value from IoT requires a thought leader who can balance technical, operational and business realities. The IoT architect role significantly increases organizational readiness for and capacity to deliver IoT.

A recent Gartner survey finds that only 31% of respondents in organizations without an IoT architect say they are technically prepared for IoT.[1] And even among organizations that *have* appointed an IoT architect, 24% still don't believe they're adequately prepared (see Figure 2 and Note 1). Such a lack of confidence in IoT competence will cause the business to avoid IT and seek a delivery partner elsewhere in the organization, engage an outside party to lead IoT efforts, or forgo business opportunities.

Figure 2. Survey: IT Preparedness for IoT



Base Total = 555
Q. Currently, how prepared is your IT organization to address these technology areas? — IoT
Q. What is the status of each of the following roles within your organization? — IoT Architect

Source: Gartner (September 2017)

Gartner defines an IoT architect as:

A technology leadership position responsible for the development and governance of the IoT target architecture and implementation strategy.

Key responsibilities of the IoT architect include:

- **Spearheading development of the IoT vision and technical strategy:** Architects play a pivotal role in understanding the needs of the business and the current capabilities of IT, while prioritizing the development of new capabilities. The IoT architect must have a deep and credible understanding of the problems that business and OT stakeholders need to solve. This understanding of organizational needs must then be translated into a vision of how IT will address those needs.
- **Designing the end-to-end IoT architecture:** A system-level understanding of all of the components — from device to organization — is essential to successful IoT implementations. IoT platform and solution providers have rich sets of technology options, but this is not the same as knowing what your organization's technology priorities are. The IoT architect must articulate a target architecture focused on the impact of technology implementation or adoption. This implementation must be scheduled to maximize value versus time.
- **Creating a process to build IoT solutions:** Business value is not created by great ideas on whiteboards. Value is created through great implementation and execution of those ideas. The IoT architect must advise and guide the solution and project teams in their adoption of the target architecture and execution of projects.
- **Leading the IoT center of excellence:** IoT solutions pierce organization groups and silos, requiring a multidisciplinary approach spanning many stakeholders. These groups must be engaged — consulted with, and listened to — and must participate in decision-making processes. This is the role of the IoT center of excellence (COE) — to bring together people from groups with a stake in the overall IoT strategy to act as "ambassadors" from their respective groups, and to support effective decision making. COEs do not recruit, organize and lead themselves — someone must provide that leadership, and for IoT COEs this function is best-fulfilled by the IoT architect.

Once an IoT architect has been identified, organizations should take specific steps to enable that individual. For example, they should:

- **Communicate their mandate, responsibilities and scope of authority:** Driving a technology strategy is a collaborative process and does not occur in secret. IT, OT and other stakeholder groups need to understand the function of the role, the scope of IoT architecture authority and who has the role.
- **Empower them to collaborate with OT, IT and business groups:** Every organization has politics — the IoT architect needs the organization's management to endorse and encourage collaboration and engagement. The person in this role needs the ability to facilitate

multidisciplinary, silo-piercing collaborations without having to play politics to get a meeting scheduled. This is one of the major drivers of the need for business acumen on the part of IoT architects — but they also require support and occasional "air cover" from their management.

- **Clearly communicate their ownership of the IoT technical strategy:** The IoT architect cannot manage the adoption of IoT technologies without the ability to govern it. Every architecture, technology consolidation or new governance effort requires communication and direction from management about the effort itself and ownership.

"Unlock IoT Success by Identifying and Empowering the IoT Architect" provides further details on the IoT architect, and its role in accelerating IoT value for the organization.

Sponsor IoT Workshops and Labs

Workshops and labs offer mechanisms to drive cross-organizational engagement in IoT, and to help spread awareness of IoT's nature and potential. What is IoT? What potential does it hold for our organization? How does this technology function? How can we build and operate IoT solutions? These and other questions can be explored in IoT workshops and labs. This will have the dual effect of improving all parties' understanding of IoT opportunities and challenges, and demonstrating IT's readiness to address them.

> Workshop leaders identify themselves as de facto thought leaders.

Workshops and labs have different objectives:

- **IoT workshops drive business engagement and awareness.** Clients usually use a workshop to drive awareness of what IoT is, and to increase cross-organizational engagement. A secondary objective is identifying and building the cross-organizational partnerships that will be required to deliver IoT.
- **IoT innovation labs drive up participation in core IoT architecture and governance processes.** These labs offer access to technology and resources, providing balance against the governance and control that is necessary for effective IoT adoption. The lab environment provides rapid access to the technology, while addressing the technology curation and standardization needs of the IoT strategy.

> Labs not only demonstrate technical skills, but also help establish architectural standards.

Some organizations combine these two concepts into a "hackathon" format. The hackathon will usually provide a ready-to-use technology set and a business problem to be solved in a semicompetitive environment. Hackathons are often sponsored as employee engagement events, but they also help demonstrate the technology and drive business exploration of IoT's benefits.

Proactively Address Organic IoT

Device and equipment manufacturers are aggressively adding new IoT functions to their products and services. Suddenly, everything from the candy machine to the elevator to your lighting needs network connectivity back to a supplier platform. This trend is very disruptive, creating significant unplanned work, because:

- **The devices and services involved don't participate in purchasing processes:** Usually these aren't new purchases, and when they are, they are often new versions of previously approved capital investments. As a result, tollgates and other governance reviews that are part of the purchasing or budgeting process are not usually triggered.
- **Simple enablement or connection of the device doesn't onboard a project:** The fact that your vending machine manufacturer would like a Wi-Fi connection doesn't result in facilities onboarding a project. This comes into IT as an ad hoc request — if the project isn't completed without IT involvement and discovered after the fact. Again, in many cases, normal network and security governance processes are not triggered.
- **None of these devices fit IT governance models:** Much of the focus of IT effort is to standardize and reduce. IT would like to support as few types of desktops, servers, applications and other IT elements as possible to meet business needs. Often security, risk and governance models are built on the assumption that these limits work. Organic IoT adoption turns this on its head, causing an explosion of the types of devices that IT, network, monitoring and security processes must be able to address.

Gartner clients across industries, from manufacturing and utilities to healthcare and commercial real estate, are experiencing this disruption. Just when everyone thought a stable approach to managing networks had taken hold, these IoT innovations came along and triggered a re-evaluation of not only networks, but security and governance as well.

> Advertising oneself as an emerging strategic partner while failing to meet current needs creates an intractable negative perception barrier.

This problem is not going away. Organizations need to evaluate how this organic IoT growth impacts:

- Security
- Network architecture
- Monitoring and support responsibilities
- Network governance
- The availability and stability of other services on the network

While no easy answers have emerged, one things is clear: Networks will have to become more robust and implement more security features (e.g., additional zones, microsegmentation and network intrusion prevention systems).

Organizations can take the following actions today to address organic IoT:

- **Communicate a process and document demand:** Are you getting one request a month or three a day? Do these requests take only a minute to fulfill or result in hours of unplanned work spread across many groups? How many teams or groups are being affected? Having data to answer these questions is key to being able to rightsize your processes and (if needed) justify automation or staff. The first step is to clarify a single process that establishes a single method for requests to be placed and fulfilled. If organic IoT requests are being fulfilled by multiple groups in networking or desktop support, or through the social network of the organization, they cannot be understood, quantified or managed.
- **Develop a simple risk classification model:** Service and governance models develop over time as an organization develops an understanding for a topic. Your organization likely already has classification models for availability, data protection and disaster preparation. These models exist to accelerate decision making and to transform items from a series of ad hoc decisions into an applied framework (with a few exceptions from time to time). Collect information about organic IoT requests and try to develop a basic model. Does your organization already have a risk classification framework? If so, that's a great place to start. If not, start by asking questions about life safety, data protection and service liability. These are the characteristics most risk and service classification models are built on, and IoT will not be an exception.
- **Track these devices:** Many of these devices will not fit into your current network device classifications, and most will not be able to meet service management, patching and maintenance expectations. Keep track of the devices and the groups that own them. Once these devices have problems, such as becoming infected by malware, how will you determine if they can be shut down? Many organizations have to go out and discover what a device is actually doing before being able to make a shutdown decision, which consumes time and resources. In the future, you will want to be able to bring these devices under better management. Keeping track of them will help justify and accelerate that process.

Organic IoT will happen. If you do not centralize the requests for network access and placement, you will not be able to justify resources or systems to support IoT.

Organizations Will Demand That IT Demonstrate Its Readiness to Execute on IoT Projects in 2018

Readiness is demonstrated by having a clear approach to delivering IoT solutions that are aligned to and prioritized by business priorities and constraints. This is the core work of IoT architecture. The essence of this work lies in the identification of business needs, the articulation of a technical strategies linked to addressing those needs, and the development of a delivery approach that project or program management can act on. Technical strategy is the tool used to address key questions about current and future capability — and it is the ability to address these questions that provides tangible evidence of readiness. This is accomplished by developing a target architecture that enables the communication of:

- Description and prioritization of business objectives as understood by IoT architecture
- The technology components required to meet various business objectives
- The business objectives that can be met now, using available architectural components
- The impact-prioritized set of skills or technologies the organization must acquire or develop
- The project, management and operational processes required to support these efforts

The technical strategy addresses execution, planning and operational concerns in a tangible and confidence-inspiring manner.

> A single IoT solution does not a strategy make. Organizations will have multiple, simultaneous, ongoing IoT projects. Failure to align these efforts to a target architecture results in technology sprawl, redundancies and inefficiencies that drive up cost, reduce quality and slow innovation.

In addition to increasing stakeholder confidence, an IoT technical strategy:

- Helps avoid technology sprawl and redundancies
- Provides context and structure for skills development
- Enables technology adoption planning
- Clarifies how existing technologies will be used in the future

Now is the time to either develop or tune up your IoT technical strategy. Organizations that are still exploring IoT, and have not yet committed to it, can use the development of a strategy to clarify the role IoT will play. Organizations that have decided to execute, or are already executing, IoT solutions need the IoT technical strategy to ensure they are on the most direct path forward.

Planning Considerations

The following practices will help IoT architects or architecture teams demonstrate their readiness to execute on mission-critical, high-impact IoT programs:

- Treat business need as your "true north"
- Develop and adopt an IoT technical strategy
- Jump-start projects with an IoT reference model

Treat Business Need as Your True North

IoT strategies focus on, and are grounded in, business objectives. IoT modifies or creates vital business functions. Organizations do not take a casual approach to changing vital business functions, and as a result they should not take a casual approach to IoT. This is a key differentiator between IoT and many other innovations. Mobile technology, the move to web applications, IaaS cloud adoption and most SaaS offerings were net-new services, or could be adopted in an isolated fashion. However, if a manufacturer, hospital or utility modifies its core service through IoT, this can create disruptions that have ripple effects.

> IoT solutions pierce organizational silos. Invest time in understanding these organizational groups. Always fall back on business need — the "true north" toward which you prioritize, organize and design.

Technical professionals should take a three-pronged approach to identifying and pursuing top business opportunities. IoT advocates and architects should regularly take time to understand:

- **Business stakeholders:** IoT requires engagement with new groups in the organization, without neglecting existing relationships. Invest time in understanding significant groups across your organization and how they service one another. Learn and use the vocabulary of these organizational business units. Understand their goals and how their success is measured.
- **Current IT efforts, particularly data analytics:** What organizations spend money on reveals a lot about them. Determine the business objectives of the top projects in IT (and other groups) across the organization and whether IoT can play a role in aiding them. Find out if they are developing technologies or datasets that are valuable to IoT efforts. Ask what information your big data team already has. An important question for big data teams is, "What data do you wish you had?" Often, IoT can fill those gaps.
- **Operational technology:** IoT solutions draw their strength from bringing IT and OT together. IoT breaks down silos between groups and brings new perspectives (and tools) to bear. This cannot be accomplished without an understanding of each of the OT groups within your organization — and often there are many. For example, a research hospital will generally have clinical engineering, facilities and specialty-group-specific technology teams, as well as teams that support research efforts. Unless your organization is a very narrowly focused one, you'll be missing something if you only engage with one OT team.

> Engagement should be accomplished though routine, long-term practice, not a one-week blitz. The credibility and presence you seek as an IoT leader builds over time — invest in it.

Keep in mind that you are trying to develop a deep understanding of not only the challenges these organizations face, but also the intellectual, operational and capital resources they can bring to an IoT effort.

Develop and Adopt an IoT Technical Strategy

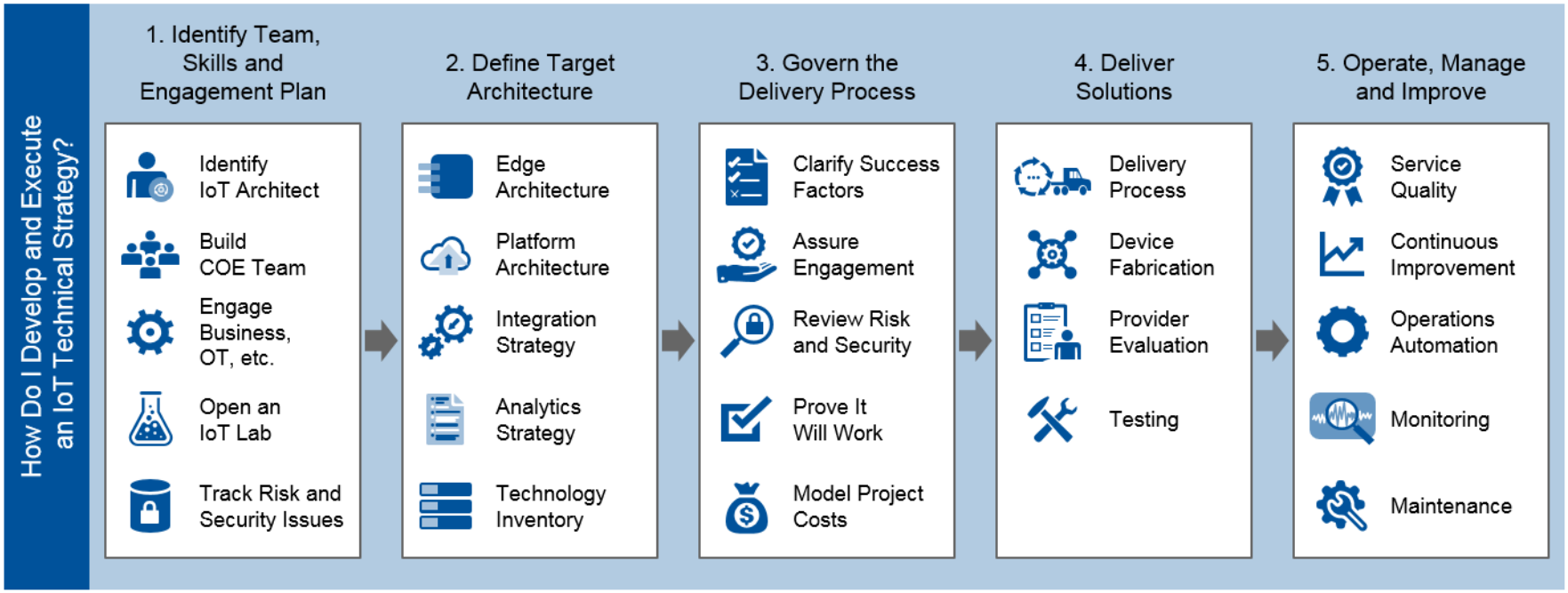
IoT is still emerging. Adoption often feels slow because "brownfield" innovations dominate IoT. As new connected products emerge, such as next-generation thermostats, doorbells or lights, these can often be adopted quickly. But innovations that involve changes to existing, complex and important systems take more planning and consideration. "Fail fast" may be the mantra of new code development, but it is not the mantra of smart cars, traffic controls, manufacturing plants or biomedical devices. Agile development methods have a place in IoT development — and are very important — but placing them in the right parts of your delivery pipeline can be tricky.

This is where bimodal approaches are transformative. "Increase Agility With Bimodal IT and a Pace-Layered Application Strategy" provides context that can be applied to IoT (and all digital business problems).

> Adopting a single process for building IoT solutions will drive commonality and make successful implementation a habit. The organizations that have a more structured approach to IoT will be more successful.

Gartner has developed a Solution Path to guide your organization from idea generation, to execution, to operation (see Figure 3 and "Solution Path for Developing an Internet of Things Strategy"). Many stakeholder objections can be addressed by "having a plan" — and the IoT technical strategy provides that plan.

Figure 3. Solution Path for Developing and Executing an IoT Technical Strategy



© 2017 Gartner, Inc.

Source: Gartner (September 2017)

Success in IoT isn't delivering a single innovation. Success is creating a culture and infrastructure that enable streams of innovations, and the increasingly rapid delivery of innovations within those streams. Your organization is probably in one of the following two spots — and should act accordingly:

- **The organization has yet to (and may not) commit to IoT:** Focus a few hours on the Step 1 tasks in Gartner's Solution Path (see Figure 3) as soon as practical. Use a workshop or exploratory meeting to empanel a center of excellence in "stealth mode" — all the group needs to know is that someone is trying to understand their needs and establish a position on IoT. What would that position be? Does the organization have pressing business objectives that could best be achieved through IoT innovation? Such sessions are often structured as workshops to explore what IoT is, and to brainstorm on how it could be applied. Be sure to capture key statements and quotes — they can be powerful "sound bites" for inclusion in later business cases.
- **The organization has made a commitment to IoT, but needs to structure its effort:** If the organization has made a commitment to proceed, you need to structure that effort for success. Note that the Solution Path is not intended to become a heavyweight program management process. The intention is to identify the tasks that will either be required or make the journey easier. Each activity should initially be approached with the goal of keeping it as simple as possible.

Innovators should always be prepared for the response: "That's a great idea; do you have a plan for delivering it?" Often, they are so focused on getting their ideas recognized that the delivery part is lacking. Leverage Gartner's Solution Path (as well as Gartner's IoT Reference Model — see below) to address decision maker anxiety and obtain buy-in.

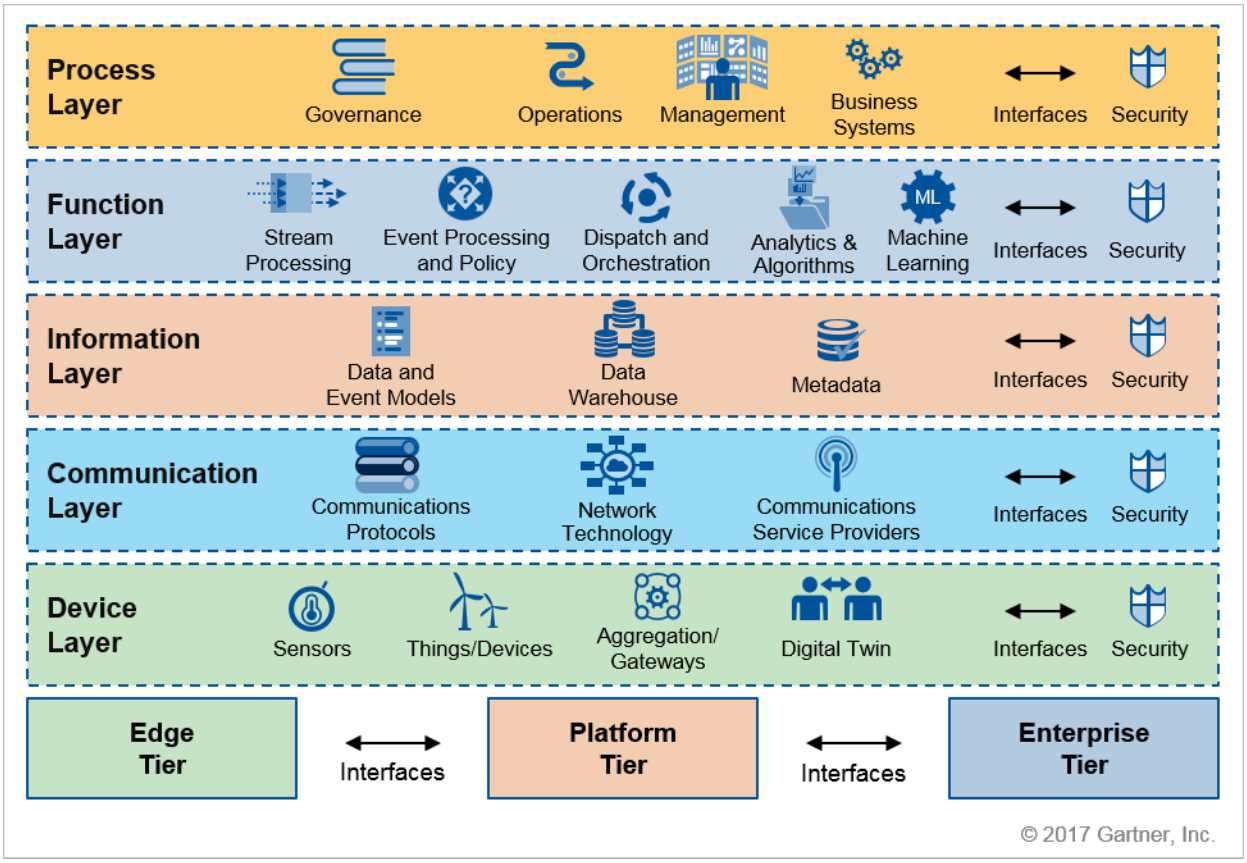
"Solution Path for Developing an Internet of Things Strategy" illustrates the details for sizing and implementing IoT technology strategy for your organization. Bimodal IT complements many of the steps laid out in the strategy, and an excellent exploration of how bimodal IT complements strategy is provided in "Scaling Bimodal — Fusing IT With the Business: A Gartner Trend Insight Report."

Jump-Start Projects With an IoT Reference Model

One common readiness-related objection from stakeholders involves the IT organization's ability to complete project and technical planning. IoT solutions are complex by nature, and stakeholder concerns in this area are reasonable. The Gartner IoT Reference Model (see Figure 4) was developed to aid clients in the sizing, planning and design of IoT solutions.

> The Gartner IoT Reference Model can also be used to facilitate technical brainstorming sessions and to drive technology workshops.

Figure 4. The Gartner IoT Reference Model



Source: Gartner (September 2017)

The Gartner IoT Reference Model provides a framework that enables technical professionals to define their system architecture. The model includes a three-step process that provides a methodology to guide technical professionals toward this goal. Organizations can use the model and process regardless of what technology they use, which vendors they select or what business outcome they are trying to achieve. This enables the model to have great relevance in both of the following cases:

- **If your organization has yet to commit to IoT:** Leverage the model to facilitate and structure brainstorming and "what if" sessions. The model is lightweight and can be used to quickly identify technical requirements for candidate projects.
- **If your organization has committed to IoT, but needs to structure its effort:** Leverage the model in all phases of IoT solution development, as it can be used to:
  - Help understand the technical requirements and scope of proposed projects
  - Size and scope efforts during project onboarding
  - Confirm a solution's technical plan once detailed requirements are signed off

- Guide post-project-delivery technology reviews

> Even organizations that are not IoT builders themselves will utilize IoT-enabled services, and must manage the technology that products and services bring with them.

Sprawl is the enemy of sustainable and cost-effective IoT. Multiple groups will likely try to implement IoT across the organization. In addition, suppliers of every type will be "IoT-washing" their products, making it difficult to understand what solution components an organization does and does not own.

> Use a mix of IoT technical strategy and purchasing discipline to manage and avoid IoT sprawl.

Many suppliers are adding IoT functions to existing products, while others are claiming IoT services that may be immature at best. Further complicating this situation are shadow IoT initiatives, in which business or operational units launch IoT solutions without engaging IT, purchasing or other collaborators.

Steps organizations can take to address this challenge include:

- **Identifying an IoT point of contact:** Even if the organization has decided to defer action on IoT, it is still important to identify an official point of contact for IoT-related issues. Ideally, this person will be the IoT architect, or someone within the architect's organization. This single point of contact can ensure that the organization isn't purchasing redundant capabilities, and can help prevent buying centers from being bamboozled by vendors.
- **Leveraging IoT target architecture:** Technology investments that use IoT as their justification should have a clear role in supporting the target architecture in terms of capability and timing.
- **Establishing a clear process:** Having a point of contact is important, but it is also important to identify what the process is for submitting an IoT innovation or purchase requests. Determine what information is needed and who this is directed to. Also, when a response will be provided. In addition to avoiding technology sprawl, IT has a role in governing the onboarding of IoT-enabled products or services. Avoid creating multiple points or vague processes, and find a single way to partner with procurement and organizational partners.

Ensuring that the IoT target architecture is leveraged to support decisions to build and adopt IoT has clear purchasing and deployment governance value. Having IoT architecture engaged with adoption provides valuable insights regarding business operations that aid in the ongoing development of the IoT technical strategy. Gartner recommends that the IoT architect have a role in both new solution development and IoT adoption.

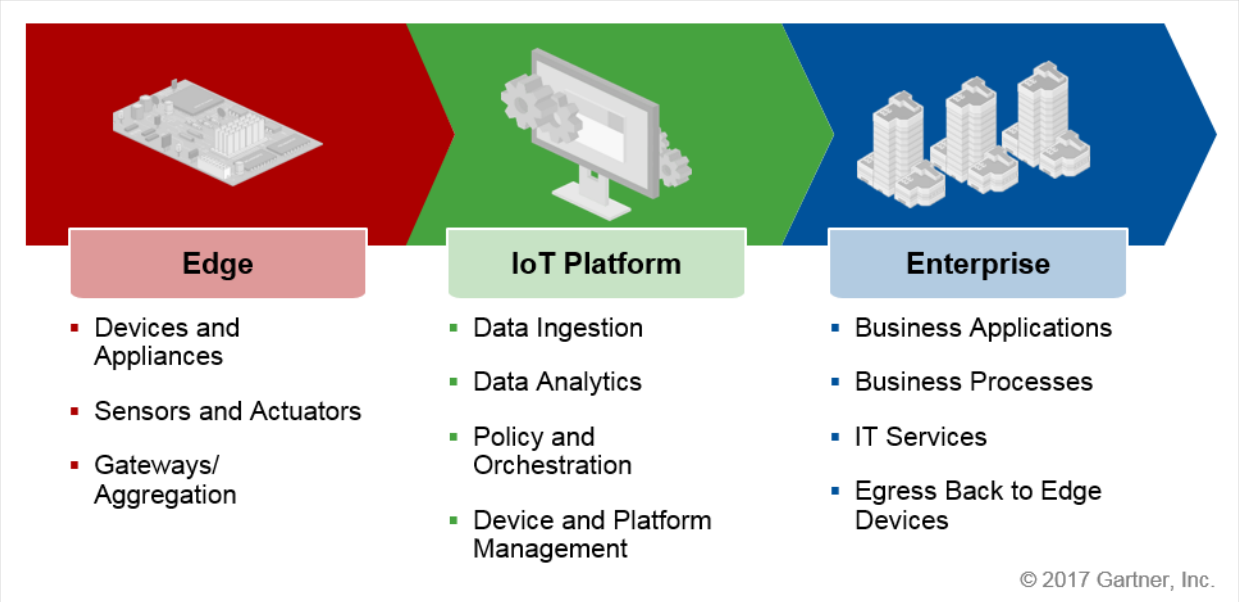
Complete details on the nature and use of the model are available in "Architect Your Internet of Things System by Using the Gartner IoT Reference Model." While the IoT Reference Model may

look like a heavyweight one, it does not have to be used that way. Agile methods have a role to play here. See "Become an Agile Superhero: Eight Attributes for Success" for a refresher on how to make agile methods work for you.

IoT Design Patterns Will Stabilize in 2018

The edge-platform-enterprise model Gartner introduced in "Preparing, Planning and Architecting for the Internet of Things" continues to be an excellent tool for modeling, designing and architecting IoT systems (see Figure 5).

Figure 5. Three Parts of an IoT Solution



Source: Gartner (September 2017)

As organizations deploy IoT to support more complex and demanding use cases, complementary design patterns are emerging. Primary among them are edge computing and unifying platform patterns. During 2018, these will become implementation styles that all major suppliers will support and reference.

> Edge computing requirements and hype are the strongest drivers for current IoT design pattern evolution.

Organizations are challenged with addressing data processing, service availability, performance and data protection within the edge environment. These requirements need to be balanced against the value of leveraging the centralized compute and storage capabilities of the platform. The hype from edge computing suppliers would lead us to believe that every IoT site in the world will become its own data center. This hype ignores the reality that the optimization or improved decision-making

capabilities of IoT often require vast amounts of information that are not accessible from edge locations.

This reality will result in the maturity of two apparently competing approaches, which will grow into one clearly defined hybrid and complementary approach. IoT as a unifying platform, sometimes called a "platform of platforms," will address the fact that platform use is not one size fits all but has the role of augmenting both edge and enterprise capabilities. There will be more compute capability used in many edge use cases, but in 2018 we will see a clarification of the design rules and the stability of various edge computing strategies.

Planning Considerations

As the building blocks for IoT continue to mature, new design patterns and problem-solving paradigms will continue to emerge. In 2018:

- The "IoT as unifying platform" pattern will dominate mega-scale industrial IoT.
- Edge computing will become better-understood, improving adoption.
- The platform market will continue to evolve along lines set out in 2017.

2018 will put several of these patterns and paradigms to the test, and separate fact from hype. A key priority for organizations planning or committed to IoT will be to track and act on these pattern developments.

Investigate the "IoT as Unifying Platform" Pattern If Your Organization Has Legacy Control Systems

Many organizations with sophisticated existing control systems are not migrating to IoT platforms, but are leveraging them as bolt-on enhancements to these systems and as epicenters for unification. This is often referred to as a "platform of platforms" pattern. Gartner expects this approach, in which IoT is used as a unifying platform, to dominate mega-scale industrial IoT.

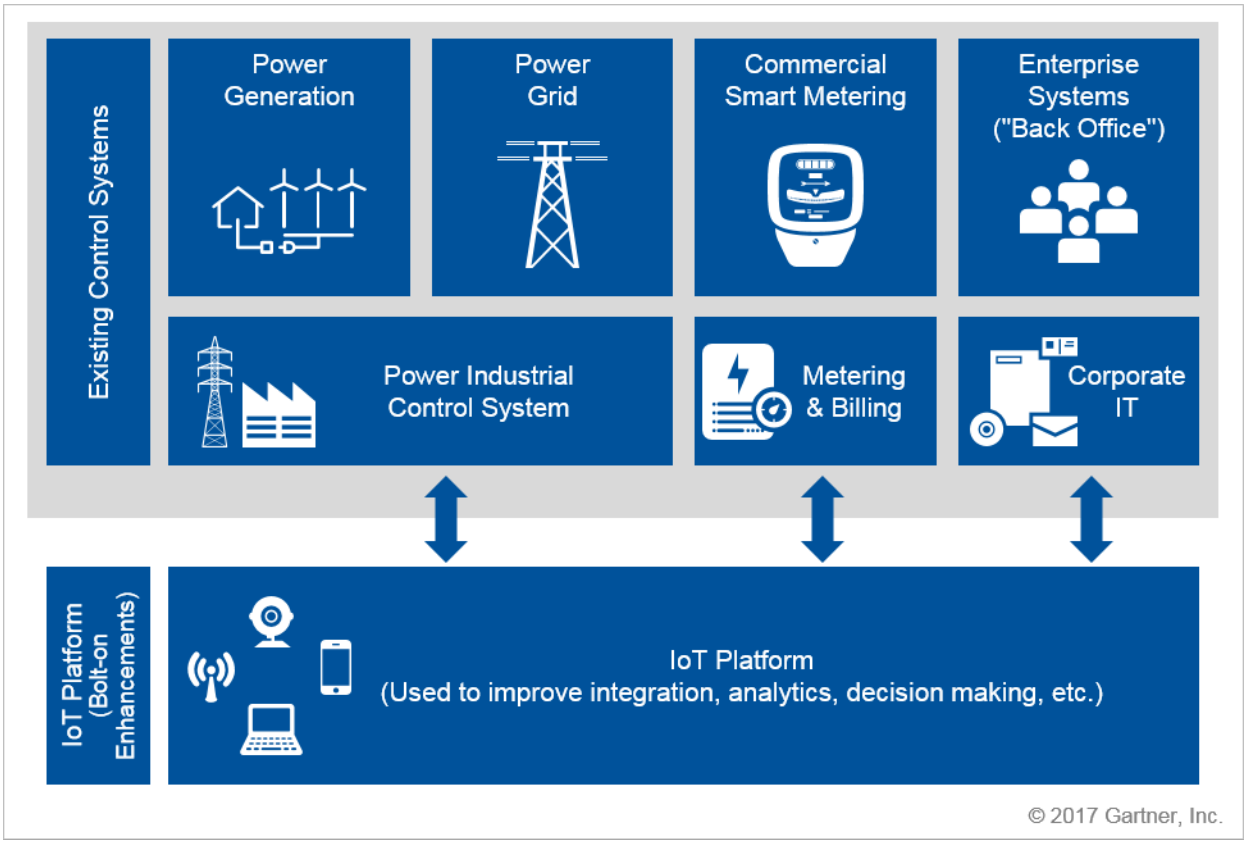
The gravity of these existing control systems comes from a number of factors, including the fact they are:

- Tested and operating today
- Currently integrated with edge control systems
- Contain business and control logic (which is difficult to extract)
- House significant amounts of historical data
- Have trained operators and support staff

> Many of the factors that give existing controls systems gravity also impede innovation. Organizations are addressing this by integrating these systems with IoT platforms.

The cost associated with migration from these systems is huge by IT standards as many industrial and manufacturing environments to have multiple control systems, even within a single assembly process or industrial function. An IoT platform can help unify them (see Figure 6).

Figure 6. IoT as Unifying Platform



Source: Gartner (September 2017)

This pattern is common in manufacturing, where a single discrete or continuous manufacturing process may have multiple mature control systems in place. IoT platforms are used to provide a unifying point for these disparate systems, and also support the deployment of new edge capabilities.

Explore Opportunities to Reap Benefits From Emerging Edge Computing Solutions

2018 will start as the year of edge computing hype, but end with organizations having a solid understanding of when and how to use edge computing.

Hardware suppliers are being presented with a tremendous opportunity as the result of edge computing needs. This is an opportunity for them to disrupt markets traditionally owned by control system providers and to take mind share they have lost to the cloud. The problem is that their hype is confusing prospective buyers.

There are a number of reasons to pursue edge computing:

- **Filtering and Transformation:** Basic data processing, filtering and message formatting are core edge functions, sometimes performed in a gateway.
- **Cycle Time:** Some tasks cannot tolerate communication latency to the cloud and back.
- **Availability:** Business-critical processes need the capability to encounter network connectivity or other service disruptions and still complete tasks.
- **Data Protection:** This priority is usually driven by intellectual property or data sovereignty requirements, resulting in the data being stored and processed within a particular control boundary — usually defined by corporate or geopolitical boundaries.

There is considerable interest in leveraging data analytics and machine learning via edge computing as well. There is a vast difference, however, between applying such models and developing them. For example, some wristwatches contain functions enabled by neural networks, but those networks were not developed on the watch.

Tasks or situations that are not well-suited to edge computing include:

- **Decisions or analysis requiring multisite or historical data:** Edge computing is unlikely to be the best choice if the data needed to make a decision requires information from multiple sites, multiple parties or is historical data.
- **Application development:** IoT functional testing requires access to testing and simulation, often with large datasets. The development and validation of analytical models requires large datasets and signification computational resources.
- **Periodic compute peaks:** If workloads have periodic tasks that require significant compute power, a strategy that purchases for these peaks will be expensive.
- **Data storage or protection:** Large datasets with retention, availability, backup and archive requirements aren't well-suited to edge computing.

In 2018, organizations should be wary of edge computing solution providers that don't clearly delineate what they *cannot* do, in addition to what they can. Beware of "snake oil salesmen" trying to solve all your problems at the edge.

Plan for Continued Segmentation and Consolidation of the IoT Platform Market

Business logic, analytics and orchestration all reside within the IoT platform. Although the platform component of IoT architecture doesn't receive as much attention or glamor as the edge does, it is the "beating heart" of IoT. The platform is the architecture component that makes things happen.

The IoT platform is also the most agile, adaptable and elastic architecture component. Changing the analytic or compute capacities within the edge often means having to redeploy or modify endpoint hardware. Cloud-based IoT platforms provide on-demand elasticity, enable agile solution development, and inherit new features and capabilities as the platform evolves.

> With over 400 suppliers now branding themselves as IoT platform providers, consolidation is inevitable — but we will see more specialization first.

The explosion of vendors identifying as IoT platform providers continues. As the market evolves, the various types of offerings in the IoT platform market will continue to segment. Specifically, Gartner expects that, during 2018:

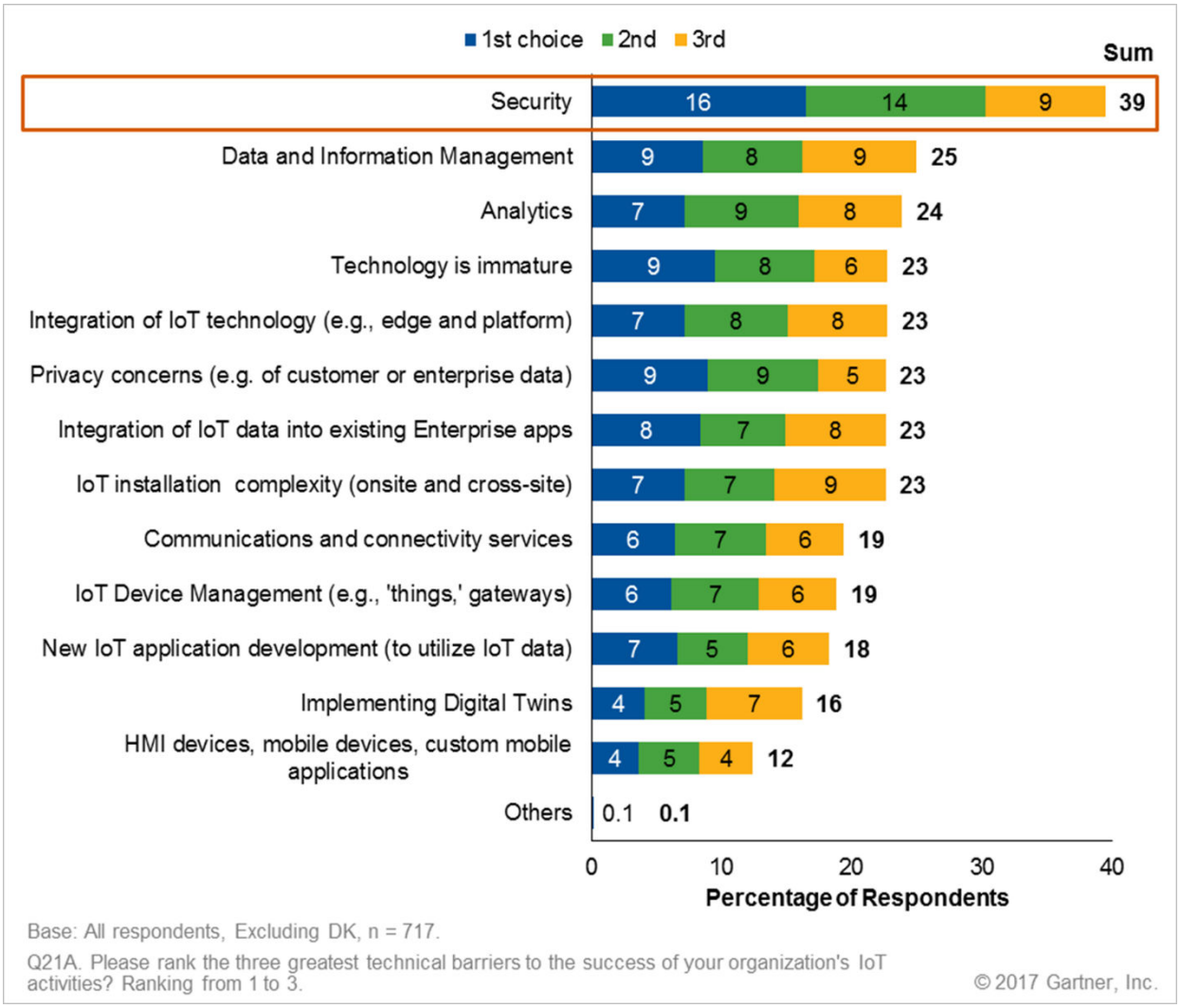
- **Hyperscale cloud providers will be the heir apparent to the platform market.** Leaders in the IaaS market have leveraged their offerings by extending them and branding them as IoT platforms. These services are general-purpose in nature, following the general market philosophy for large-scale cloud service providers. We expect Amazon Web Services, Microsoft Azure and IBM Watson IoT to be very dominant in this space.
- **Strong "platform plus" offerings will become more prominent, but will not yet lock down their markets.** Platform-plus services enhance general-purpose IoT services with improved tooling, targeted intellectual property, or both. GE Predix and PTC ThingWorx were early adopters of this approach, and more players are entering the market. Often, this an attempt for an organization to maintain existing strategic relationships with edge equipment users, and to avoid disruption from hyperscale providers moving into previously closed markets.
- **Niche solutions providers will continue to emerge.** Also emerging are providers that have no intention of competing based on core platform functions. Instead, they are entirely focused on solving one piece of the puzzle, such as cellular device management or service monitoring.

This raises an interesting problem: Platform-plus and niche solution providers often depend on, and partner with, one or more hyperscale cloud provider for their infrastructure. As a result, their infrastructure partners are also their competitors. Even more puzzling is the long-term strategy for many of the smaller products in the space — some of which are being developed by large organizations that have natural rivalries with the hyperscale providers. In many cases, the platform-plus and niche solutions cannot be valuated based on the sale of the product, because the only viable buyers are competitors. This all will add up to orphaned products. Gartner expects significant market consolidation, but given the current strong U.S. economy, this will likely be delayed until 2019.

Proactively Addressing Risk and Security Will Continue to Be a Top IoT Priority

Gartner's IoT research consistently finds that organizations cite security as a top implementation concern (see Figure 7 and Note 2). Nearly two in five (39%) of the organizations surveyed identified security as one of their top three barriers to IoT, and this is similar across countries and verticals. IoT innovations revolutionize or create vital business functions, and organizations are keenly concerned about protecting these assets. Often, that protective concern expresses itself in security terms, but clients also express significant concerns about their ability to deliver, run and maintain IoT systems.

Figure 7. Top IoT Concerns



Base: All respondents, excluding "don't know," n = 717.
Q: Please rank the three greatest technical barriers to the success of your organization's IoT activities. Ranking from 1 to 3.

Source: Gartner (September 2017)

Planning Considerations

Risk continues to be a major obstacle to IoT adoption. Information security is a major component of this challenge, but is not the entire story. Key planning priorities for 2018 include:

- Address testing and service quality questions before they are asked.
- Leverage the privacy, safety and reliability (PSR) model to identify specific risks.
- Focus on immediate security priorities.

Address Testing and Service Quality Questions Before They Are Asked

IoT innovations often involve unique assets. For example, there is no test city, with traffic lights, police and public works, in which to perform preproduction "smart city" testing. Individual components can be tested, but there is no way to perform full end-to-end testing of a smart city — or a power grid or assembly line, for that matter. All of these assets contain expensive singleton components and lack isolated test environments. If you are advocating for an IoT innovation in such an environment, be prepared to discuss how you will ensure innovation without catastrophic disruption.

> IoT innovations modify or create functions vital to customer service and operations — often involving expense and unique assets for which there are no nonproduction or test versions.

What components should you include in your testing and service quality planning? Here are a few pointers:

- **Begin with your current toolset.** Ascertain what testing and monitoring tools exist in your organization today. Note that this consideration doesn't just include tools within the IT organization. OT teams have testing and monitoring capabilities, so invest time in understanding them.
- **Instrument the environment to detect failures immediately.** Examine your end-to-end architecture and monitor each component's availability and performance. Include information about *when* the data was captured, and be sure you can identify when endpoints stop reporting or become delayed. Plan for pulling logs and system alerts back to a common, single point of analysis.
- **Unit testing is key.** Unit tests are not only useful in development, but they can also be used in quality assurance to ensure that the entire set of components in the system is working properly.
- **Enable network captures and simulations:** Develop the capability to capture and play back data streams, and to run full-scale simulations of key components of the system.

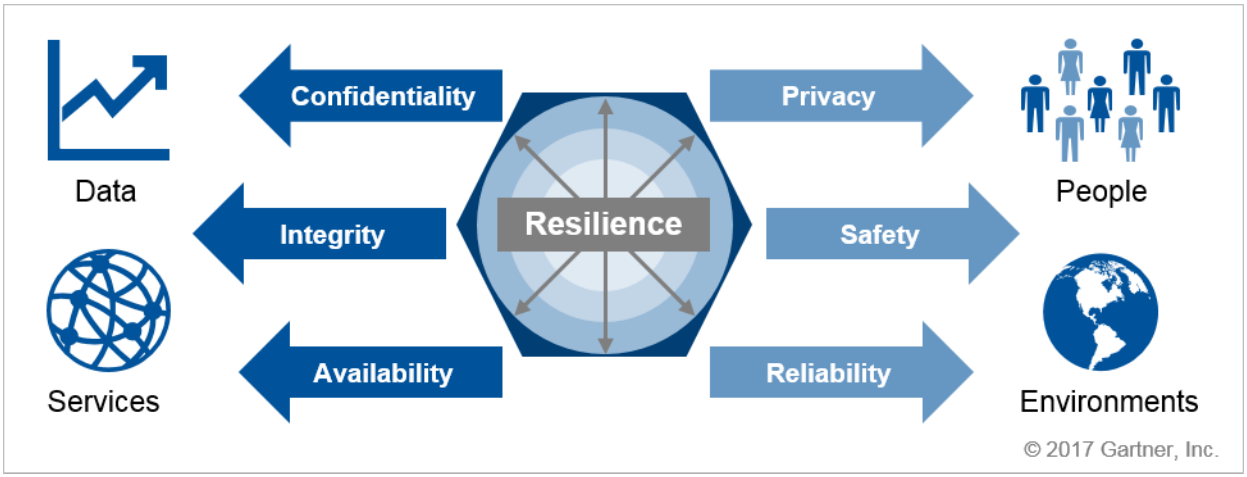
If your organization has not yet committed to an IoT strategy, limit your investment in time and have a very basic plan. There is an enormous difference in stakeholder perception between a plan that outlines issues that will have to be addressed and how versus no plan at all. Conversely, if you are

in an organization that is spinning up an IoT program, you need to nail down these details and drive testing and service quality expectations into every aspect of solution development.

Leverage the PSR Model to Identify and Rate IoT Risks

The PSR triad covers the environmental and people-related risks of a digital business solution (see Figure 8). It is used alongside the confidentiality, integrity and availability (CIA) triad to create a bridge between digital business risks and the security controls that can be used to address risk in various processes and technologies. Gartner finds this dual model to be better-suited to modeling IoT risks than the traditional CIA model alone.

Figure 8. The CIA-PSR Model for Resilient IoT Solutions



Source: Gartner (September 2017)

The central element of this approach is the concept of resilience. International Organization for Standardization (ISO) 22316, "Security and Resilience — Organizational Resilience — Principles and Attributes," defines resilience as "the ability of an organization to absorb and adapt in a changing environment, to enable it to deliver its objectives and to survive and prosper."[2] Resilience is critical for IoT systems.

When applying this model, begin by identifying overarching organizational objectives related to each of the three PSR risk categories:

- **Privacy:** This is a people-related corollary to confidentiality, which is generally evaluated in terms of what data you are obliged to protect. Privacy is much more subjective. There may be regulatory or contractual obligations related to privacy, but in the context of the PSR model, privacy is evaluated from the perspective of individuals. What were their expectations regarding the protection of the data? From a privacy perspective, there are many legal and ethical uses of data that can still cause people to feel unsettled or disturbed.

- **Safety:** Integrity focuses on the basic question of whether a system can be trusted to operate as expected. Safety takes this a step further, examining not only whether a system will operate as designed, but also whether technical or procedural controls are in place to sufficiently protect life and property. All washing machines, for example, contain a switch that cuts the power to the motor if the door is opened in order to protect users from being injured by the moving parts. Do you need to address end-user safety concerns? Can the system be resilient such that it fails into safe states?
- **Reliability:** When the availability of the system is challenged, how does it respond? Does it turn itself off or change to a reduced function set? Or does the system lack the ability to detect failure? Often, organizations separate disaster recovery from high availability in an effort to differentiate infrequent but profound failures from routine and anticipated ones. Similarly, reliability extends these considerations by asking questions such as:
  - How will the business operate in the event of a communication or a system component failure?
  - Will the IoT solution have the capacity for continued operation?
  - What impacts on users, clients and the business must be planned for?

Gartner recommends using the CIA-PSR model in an ongoing and continuous manner, rather than in a single-point-in-time system assessment. Build consideration of the PSR components into discussions about the business objectives of the overall IoT solution, and sensitize members of the architecture and technical teams to identify and document these issues as they come up.

Focus on Immediate IoT Security Priorities

What steps should organizations take now? Current and prospective innovators and adopters of IoT should:

- **Develop core edge security skills:** Most IoT security challenges stem from the edge, either due to the vulnerability of specific IoT endpoints, operational information that is collected, or the new actions IoT enables there. Begin by focusing on understanding how edge devices can be hardened, how network controls can be used to compensate for noncompliant devices, and how these device populations will be managed in your existing tools (or what limits prevent that). Linux is the dominant operating system running on IoT endpoints. If the organization does not have specific expertise in hardening, vulnerability management, patching and secure application development on Linux, now is the time to start developing that expertise.
- **Use a risk register to track IoT risks, even if management is deferred to a later date:** Risk registers are the cornerstone of credibility for any risk management effort. They allow you to get credit for the issues you are sorting out, and prevent items from slipping thought the cracks. They don't need be complex to be effective. Managing risk is central to effective IoT implementation and operation. Taking the time to understand how to use a risk register, even at the project or solution level, can greatly improve your risk management practices and credibility. Furthermore, understanding how your effort may be able to leverage existing organization, operations or IT risk registers may allow you to piggyback on those risk management efforts. For more information, see "Three Steps to Creating a Simple IT Risk Register."

- **Assume a "findings not just facts" perspective on data protection:** Often, the facts that are collected in IoT systems aren't themselves confidential, but a basic analysis of those facts can review restricted or confidential data. For example, the paint robot supplier for an automaker may have data on colors of paint applied, physical outlines of parts, and the number of parts painted. These facts in isolation may not be secrets, but these same facts, taken together, may leak production data and details that directly tie to revenue and profit. Most current data classification and protection approaches focus on individual facts, but IoT will demonstrate a necessity to also focus on the findings that an analysis of that data reveals. This will cause a sea change in how information security, insider threat and data governance programs operate across industries and into those industries' suppliers. Start having "findings not just facts" conversations with risk and security groups now.
- **Treat security as a multidisciplinary undertaking:** IT organizations must define an operational model to ensure successful adoption of IoT strategies and solutions, including security policy. Security policy cannot be developed in a vacuum; it will require the participation the chief information security officer (CISO), risk experts and any technology groups affected by policy or control statements. IoT endpoints and solutions don't fit into corporate security frameworks designed for managing desktops or servers. Anticipate that developing IoT policies and standards will take multiple iterations as IoT implementations take shape over time.

Setting Priorities

The IoT needs of organizations vary widely, and it is possible that different aspects of the same organization can be confronted with different needs. Gartner has identified three different priority sets to reflect this fact. Some organization may find they are in all three places at once: These are not intended to be mutually exclusive, but are instead organized to align to the challenge at hand.

Priorities for managing the demands of organic IoT adoption:

- **Centralize IoT onboarding and activation:** Ad hoc requests to enable third-party IoT solutions via corporate networks are increasing. These requests are often overly simplistic and contain hidden risks, as the requestors many not understand the implications of enabling a particular function or the resulting data sharing. To better understand the volume and nature of these requests, Gartner recommends creating a centralized point of contact and lightweight initial process. This will enable these request to be fulfilled, as appropriate, and understood. It will also allow the volume and nature of the work required to address these requests to be planned for and documented.
- **Leverage the PSR-CIA model to understand risks:** IoT is complex, and the risk implications of IoT systems can be difficult to understand. Leverage the PSR-CIA model to drive better conversations and analysis of IoT safety and security risks. Organizations have to understand the risks that are presented to them, as the result of their operations, constraints and needs. Improving the risk identification, analysis and remediation capabilities of organizations is a subject much bigger than IoT itself. Don't wait for perfect models — they aren't coming.

Priorities for organizations that are exploring how to benefit from IoT, but have not yet committed to developing IoT solutions:

- **Leverage an IoT architect to demonstrate readiness:** The single most significant way to demonstrate readiness to execute on IoT to stakeholders is to identify and empower an IoT architect. Much of this value comes from having an identified point of contact. Many stakeholders or potential project sponsors simply won't know how or with whom to engage, leading to the appearance of disorganization. If an organization is reluctant to even name a specific individual or team as a point of contact, its commitment to IoT is easy to question, and it is unlikely to inspire confidence in its ability to execute.
- **Engage with stakeholders now and document their needs:** Business needs are the "true north" by which IoT must be navigated. Science-experiment-style projects don't materialize into products or production processes with sponsors, advocates and supporters from the business. This is especially true for IoT. The business processes that IoT seeks to improve are owned outside IT, so IoT cannot be an internal-IT innovation.
- **Develop a "straw man" IoT target architecture:** The bad news is that as soon as you document an architecture, it will draw criticism and critiques. The good news is that the existence of the architecture provides structure for those conversations. No architecture is or will be perfect. The goal of the architecture is the optimization and effective execution of technical strategy. Communicate a target architecture early, provide time for feedback and evolve the architecture over time.

Priorities for organizations that have committed to IoT, and would like to maximize their IoT solution investment:

- **Develop IoT technical strategy and the process for ongoing refinement:** No technology architecture can be carved in stone, unchanging and permanent. Architectures, frameworks and strategies must be stable, but allow for evolution and refinement. The challenge is structuring and planning periods of feedback and refinement to avoid constant change. Build processes that collect feedback and identify limitations of the current IoT architecture over time. Preidentify the times during the year that changes will be made and updates will be communicated.
- **Make testing and service quality top IoT priorities:** IoT systems are too important to be unreliable. IoT innovations occur on systems that are vital to organizations and are often critical infrastructure for society. The service quality of such systems is essential to their success. Develop foundational testing, monitoring and problem resolution capabilities now to be poised to address these concerns.
- **Examine and leverage emerging IoT design patterns:** How edge and platform technologies are leveraged and developed into IoT solutions will continue to evolve for some time. Web technologies are over 20 years old and continue to see periodic advancements. IoT will be no different.
- **Monitor the IoT platform market to identify opportunities and manage disruptions:** Given the large number of participants in the market and its nascent nature, organizations should anticipate significant changes in the form of acquisitions and market failures. Many smaller or

niche providers, even some with great technical merit, will not find sufficient revenue to survive. This is one of the many drivers causing organizations to leverage existing strategic partners for IoT platforms rather than embarking on IoT with new suppliers.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Unlock IoT Success by Identifying and Empowering the IoT Architect"

"Solution Path for Developing an Internet of Things Strategy"

"Architecting and Planning for IoT Success: A Gartner Trend Insight Report"

"A Primer for Building Resilience and Security Into Internet of Things Solution Architecture"

"Architect Your Internet of Things System by Using the Gartner IoT Reference Model"

"A Guidance Framework for Architecting the Internet of Things Edge"

"A Guide to Deploying IoT Analytics, From Edge to Enterprise"

Evidence

[1] "Unlock IoT Success by Identifying and Empowering the IoT Architect"

[2] "ISO 22316:2017(En): Security and Resilience — Organizational Resilience — Principles and Attributes," ISO

Note 1 Gartner Survey

Gartner surveyed technical professionals about their organizations' technology objectives, challenges, preparedness and future plans to provide an overview of how they are dealing with changes related to digital business.

The research was conducted online from 30 March 2017 to 2 May 2017 among 555 respondents, primarily located in North America. A subset of Gartner for Technical Professionals seatholders were invited to participate.

Respondents were required to be a member of their organization's IT staff or department (or serve in an IT function). Furthermore, they could not serve as a member of the board, president or in an executive-level or IT leadership position.

The results of this study are representative of the respondent base and not necessarily the market as a whole.

Note 2 Gartner Survey

Results presented are based on a Gartner study conducted to gain insight about trends among adopters of IoT. The research was conducted online during June to August 2017, among 717 respondents in four countries: Germany, Japan, the U.K. and the U.S.

Respondents were required to have knowledge about their organizations' IoT-related business objectives, strategy and benefits. Respondents were also required to have a high level of responsibility in IoT decisions that span determining business objectives, setting the IoT strategy, and measuring or determining how to measure the ROI or effectiveness of IoT initiatives.

Quotas were established by country to ensure a good representation in the sample. A good spread of industries and company sizes was also required.

The survey was developed collaboratively by a team of Gartner analysts who follow the market and was reviewed, tested and administered by Gartner's Research Data Analytics team. The results of this study are representative of the respondent base and not necessarily the business/market as a whole.

More on This Topic

This is part of two in-depth collections of research. See the collections:

- Implementing and Executing Your Internet of Things Strategy: A Gartner Trend Insight Report
- 2018 Planning Guide Overview: Thriving in an Era of Change

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

© 2017 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the Gartner Usage Policy posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."