2017 Planning Guide for the Internet of Things

Published: 13 October 2016 **ID:** G00313353

Analyst(s): Erik T. Heidt

In 2017, the Internet of Things will move from "what" to "how" as organizations rapidly act to capitalize on new business opportunities. Technical professionals must have a plan ready to go — at a moment's notice — to address IoT business value, architecture, technology, skill sets and governance.

Key Findings

- Business interest will bring new urgency for Internet of Things (IoT) planning in 2017. Many organizations are already struggling with unmanaged adoption and shadow projects. IT must understand and proactively plan for the delivery of IoT solutions.
- The IoT architect is emerging as the central, linchpin role for planning, executing and governing IoT. Organizations are including IoT architecture, planning and execution roles in 2017 staffing and skills planning.
- Cloud IoT platforms continue to evolve rapidly. This market will segment in 2017, with general-purpose providers offering platforms that can cover general-purpose use cases, and specialty providers focusing on niche markets that have specific technology, industry or operational needs.
- Security and risk concerns will continue to be the greatest impediment to IoT adoption. The market for IoT-specific security solutions will dramatically expand in 2017 as existing security providers aggressively retool existing capabilities to address IoT security risks.

Recommendations

- Establish your organization's target architecture for IoT. This target architecture is essential for the evaluation of IoT edge and platform technology providers, and it enables effective planning and execution.
- Prepare for the screening and evaluation of IoT partners and business solutions. Many suppliers will attempt to reposition and "IoT wash" their existing solutions. Engage with business, operational technology and IT groups to ensure effective sourcing decisions.

- Make the case for a dedicated IoT architect role now. Identify and communicate responsibility for IoT architecture within the organization. A centralized perspective on opportunities, architecture, and process leads to more efficient and effective execution.
- Include security and risk modeling early in IoT solution design to enable planned remediation. Security is most expensive when organizations address it as an afterthought.

Table of Contents

List of Figures

Internet of Things Trends

More than any technology initiative of our time, IoT is business-driven. As business executives and non-IT organizations realize the potential benefits of IoT solutions, they will either compel IT groups to participate or simply move on without them. Hence, 2017 is the year that IoT moves from "what"

to "how" — and the year that technical professionals must be able to demonstrate their readiness to plan, execute and operate IoT solutions.

> By 2020, Gartner predicts that the world will contain more than 20 billion IoT devices, generating trillions of dollars' worth of business value.[1]

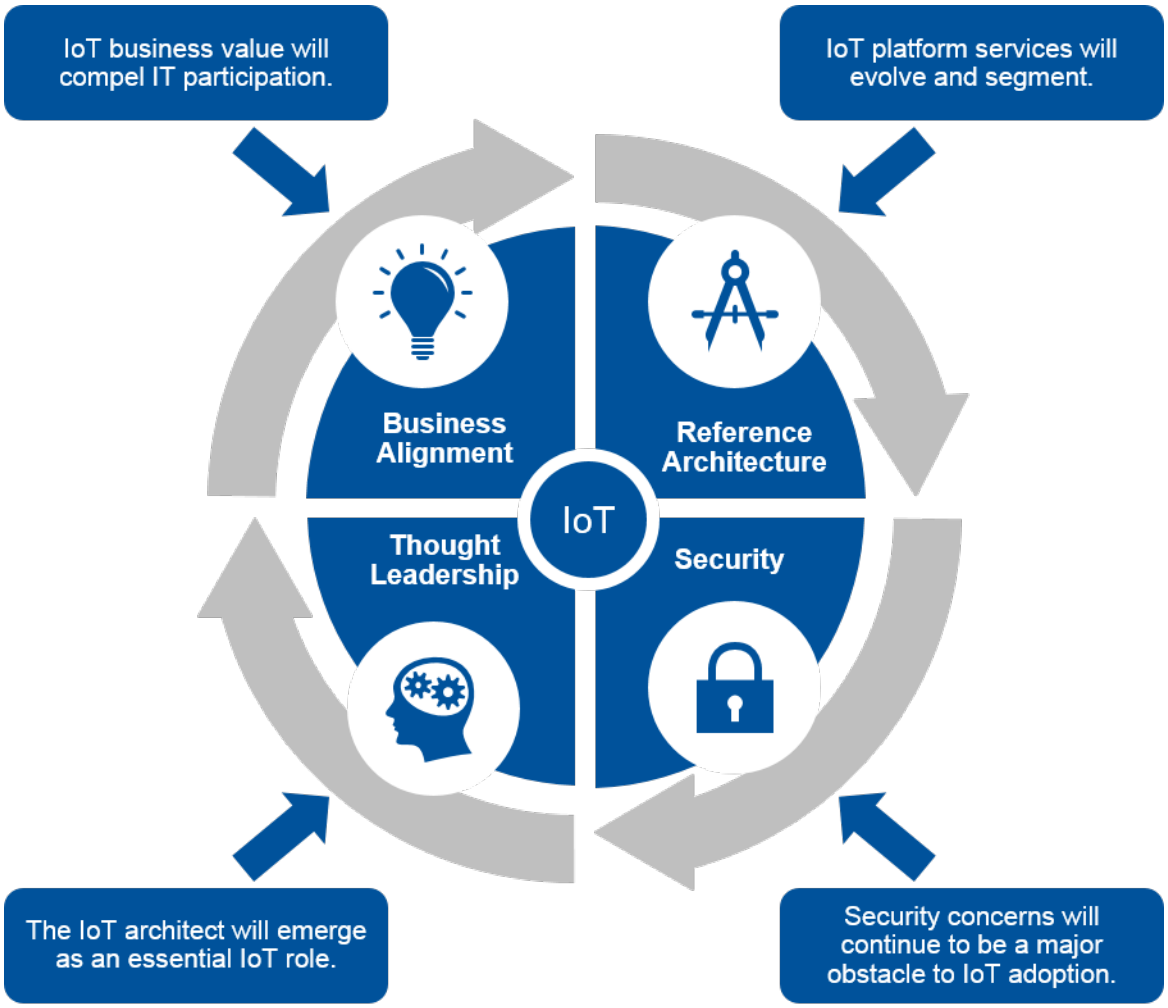
A wide range of organizations and industries are demonstrating dramatic results now. Organizations are communicating and advertising these successes — often identifying them as strategic advantages. These examples often demonstrate new value or efficiencies in areas that have been stagnant for extended periods. The result is unprecedented business interest.

Business leaders are rapidly shifting their IoT focus from "what" to "how." Technical professionals must be prepared for conversations about how to deliver IoT that inspire confidence from these business leaders. This is not the same as having a detailed plan that accounts for every conceivable obstacle. Business and sponsor perceptions about the IT organization's readiness will determine IT's role in the enterprise's IoT efforts.

This Planning Guide identifies key IoT trends and planning considerations that technical professionals must understand and address to ensure that the IT organization is not caught unprepared and that it can articulate a clear path forward (see Figure 1). The guidance in this document focuses on the following four trends:

- **IoT business value will compel IT participation.** The tide of business demand is rising quickly. IT will have a role in the organization's IoT strategy. But what will that role be?
- **IoT platform services will evolve and segment.** IoT platform services, and their markets, will evolve and segment in the coming year. IT professionals will need to leverage their organization's IoT target architecture to identify long-term partners and solutions.
- **The IoT architect will emerge as an essential IoT role.** IoT is a technical evolution that triggers organizational revolutions. Maintaining business alignment and focus requires a thought leader who can balance technical, execution, operational, and business realities and drive toward success.
- **Security concerns will continue to be a major obstacle to IoT adoption.** Security must not be allowed to derail value generation, or be addressed as an afterthought. IoT security should be addressed in a structured and direct manner. An understanding of business objectives and IoT architecture enables risk-aware adoption of IoT.

Figure 1. IoT Planning Trends

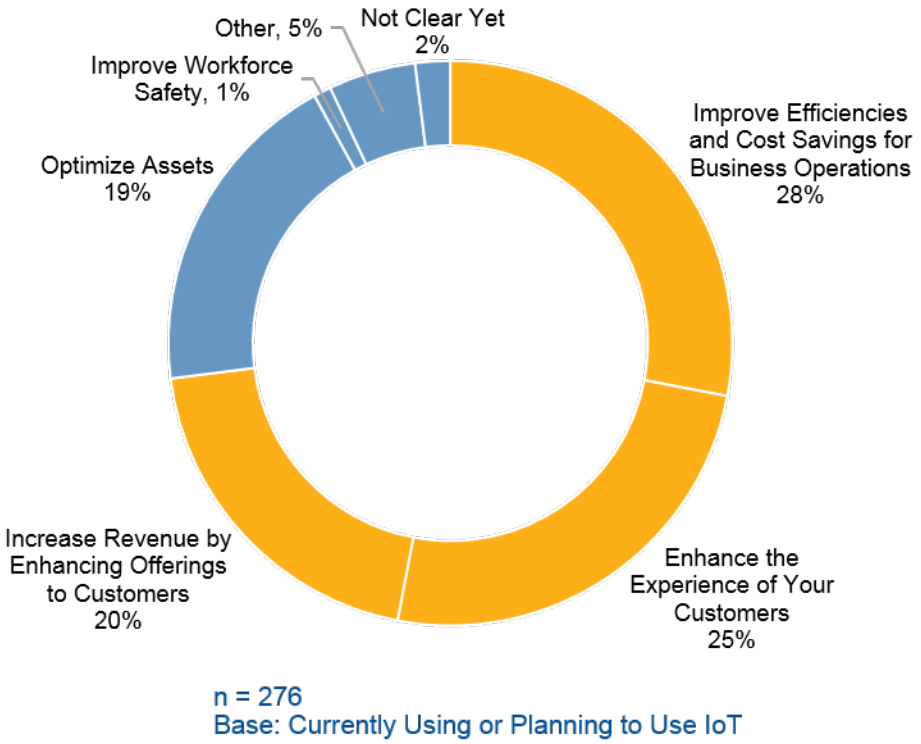


Source: Gartner (October 2016)

IoT Business Value Will Compel IT Participation

Business awareness and the desire to reap business value from IoT will increase in 2017 as enterprises seek to use IoT to drive new sources of revenue, gain cost and efficiency benefits, and improve customer experiences (see Figure 2). In the process, the short-term role of the IT organization will be determined: IT will establish that role either in a proactive manner or in response to business-led initiatives. Will IT be a partner, driving business value, building an IoT architecture and collaborating on "greenfield" projects? Will IT support the purchase of services that include IoT? Or will IT take a wait-and-see approach instead?

Figure 2. Business Objectives for Current IoT Projects



Source: Gartner (October 2016)

Many organizations are struggling with shadow adoption of cloud and mobile technologies, thereby inheriting technology components and supplier relationships. To avoid a repetition of this challenge with IoT, Gartner strongly recommends that IT get out in front of this trend now and engage proactively.

> Many IT organizations failed to get involved with SaaS and mobile technologies early. They inherited a mixed bag of suppliers and solutions that have proved difficult to integrate and support. Proactive engagement is the key to avoid repeating this cycle with IoT.

There are several mechanisms that can inject IoT into the organization. Technical professionals should consider each of these to understand how IoT will be thrust on IT:

- **Shadow IT:** This rises when business units act unilaterally, committing to or deploying solutions before engaging with IT — or avoiding IT altogether until something breaks. The major challenge with shadow projects of all types is that they often fail to account for security, service quality,

business continuity, maintenance and operational considerations. As a result, IT is often tasked with refactoring or migrating the solution or having to support yet another nonstandard technology.

- **Retrofit:** Many organizations have solutions in place that have unutilized IoT capabilities, or else new IoT capabilities that are being added by the supplier of that system. These systems pose a looming integration challenge for many IT departments. This situation poses many of the same challenges as shadow IT because the business must decide whether to forgo the capabilities, accept them as they are, or consider a costly transition to a different solution.
- **Greenfield:** Even when IoT solutions are developed by IT, they don't often start with a blank sheet of paper. More often than not, IoT solutions are efforts to improve existing systems and operations, rather than to create brand-new products or processes. The "things" — such as assembly lines, buildings, clinical systems or products — typically already exist, and there are practical limitations to how much change can be made as IoT is injected into them.

Many clients report that all three of these IoT introduction mechanisms are happening simultaneously. Increased interest in IoT is causing many organizations to adopt new perspectives on existing operational technologies.

Planning Considerations

Essential elements for success include devising and communicating a plan for addressing the IoT needs of the business. In 2017, technical professionals must:

- Drive the identification of IoT opportunities
- Identify the IoT target architecture
- Address process and governance questions

Drive the Identification of IoT Opportunities

Participating in business opportunity ideation has multiple benefits. This type of early engagement allows IT to take the role of facilitator, thus avoiding business perceptions that might drive shadow IT or IT avoidance. In addition, early engagement allows IT to understand and plan to address business needs proactively.

IoT solutions are business-driven, and IoT inserts itself into the organization as few technologies can. IoT is all about either sensing something in the business realm or making something happen in it. IoT closes the loop between "corporate" and "field" operations and cuts across fiefdoms as it does so. Smart buildings, for example, drive collaboration between IT, corporate leadership and facilities, thereby breaking down silos. Retail IoT projects provide marketing, logistics and pricing with instant data, and they enable instant action. It is difficult to identify any IoT innovation that does not pierce silos and compel new collaboration among diverse business groups.

It is important to engage with these diverse groups to identity potential business value from IoT. One key to gaining their participation and support is to clearly articulate the value of the innovation. Gartner has crafted a basic IoT value spectrum that is useful for stimulating conversations about IoT

value (see Figure 3). We recommend that IoT planners leverage this spectrum to explore and understand opportunities that present themselves to the organization. Although this spectrum is not intended to be all-encompassing, it is useful for characterizing the majority of IoT initiatives that we have studied.

Figure 3. IoT Value Spectrum

Source: Gartner (October 2016)

Identify the IoT Target Architecture

Defining the target architecture for IoT enables planning of not just technology, but also skills development. A one-size-fits-all architecture is not the objective. Rather, the goal is to select an edge and platform target state that is "one size fits many" in nature. The target architecture can then be used to guide skills development, technology adoption and supplier selection. This, in turn, enables IT to develop a schedule for when various capabilities will become available to the organization.

Gartner has identified a set of IoT capabilities within the logical architecture for IoT solutions. There are four major elements, each of which may have existing cross-over uses in the enterprise that technical professionals can leverage (see Figure 4):

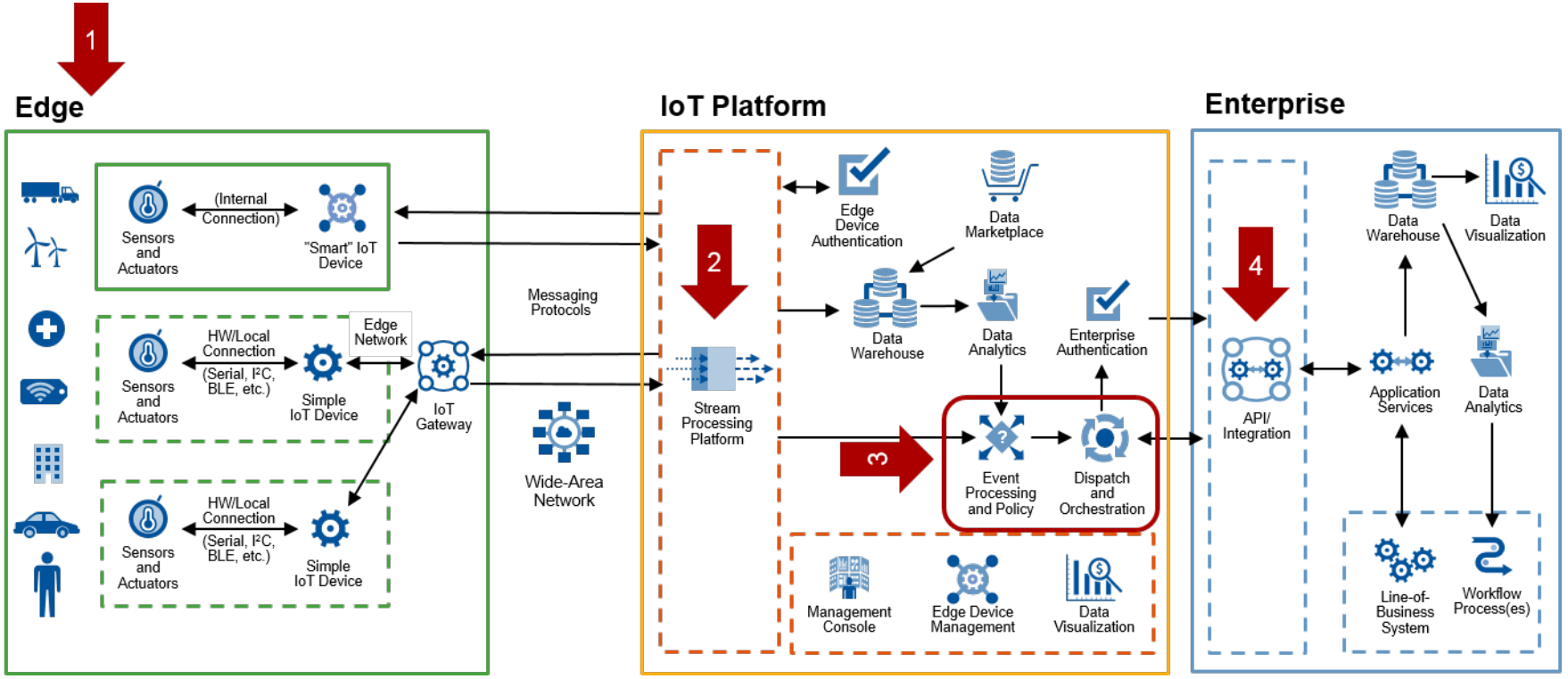
1. **The edge:** Although the edge and its associated sensors, actuators and gateways may be new territory for IT, it is the primary "stomping ground" for most operational technology (OT) groups. Such groups can be tricky to identify within an enterprise. This is because many of them — including industrial automation, clinical engineering, facilities and physical security groups — don't self-identify as "operational technology," even though they manage, maintain and run operational equipment. It is important to open channels of communication between IT and these groups now. If your organization has a clear edge environment (such as a plant for a manufacturer or retail floor space for a merchandizer), do not wait for the business to prompt engagement. Lead the charge and lay a foundation for future collaboration.
2. **Stream processing:** Big data systems share with IoT a need to ingest a large volume, variety and velocity of data. This drives the need for stream processing. Data analytics is essential to unlock the value of many, if not most, of the data streams that pass though IoT solutions. Identify whether your organization is using a stream-processing platform now and whether that platform has capabilities that can be leveraged for IoT. In addition, investigate whether your

organization has developed any subject matter expertise in stream processing in support of big data (or other) initiatives, and identify whether common tooling opportunities exist between these efforts and IoT. If the organization is not currently using a stream-processing platform that can be leveraged for both big data and IoT, try to identify suitable common-function tools that can be adopted.

3. **Event processing, policy, dispatch and orchestration:** This element focuses on logic and workflows. It comprises the functionality that is core to IT automation of most business processes. Investigate opportunities to prepare for IoT by improving the organization's core IT capabilities in this area, as well as to extract value from these components now.

4. **API integration:** Because IoT focuses on driving action and interaction between enterprise applications and the physical world, integration with enterprise systems is essential. This is another area that is core to achieving many IT objectives, where existing API integration solutions and expertise can be leveraged and expanded for IoT purposes. Integration is key to value generation. It connects internal systems to one another, to client systems and to third-party service providers.

Figure 4. Logical Architecture for an IoT Solution



Source: Gartner (October 2016)

Your organization is likely to have existing skills and technology initiatives related to many, if not all, of the key architectural components used in IoT solutions. For more information on IoT architecture, see:

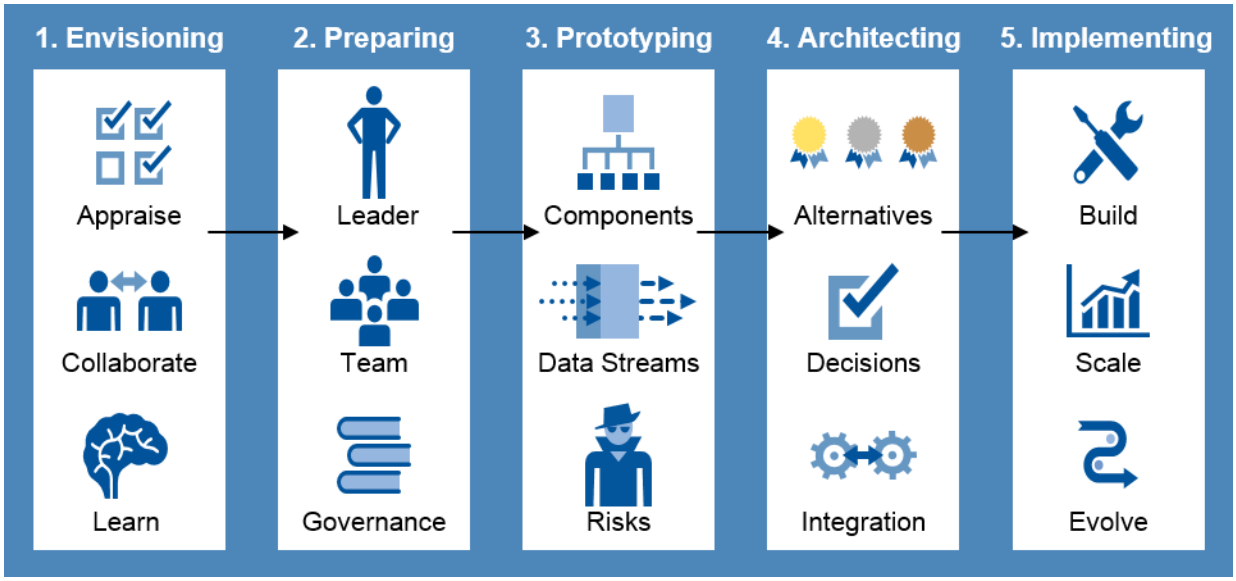
- "Preparing, Planning and Architecting for the Internet of Things"
- "Assessing Integration Architecture for Internet of Things Solutions"
- "Leverage Intelligent Gateways in Your IoT Architecture"

Address Process and Governance Questions

When organizations embark on new efforts, concerns emerge around their ability to execute not only technical details, but also planning, delivery and operation. Clearly addressing the technical details is necessary for successful execution, and it increases organizational confidence. But it is equally important to structure the overall effort, decomposing it into elements and activities with clear and attainable objectives.

"Solution Path for Executing an Internet of Things Initiative" provides a structured approach to the entire IoT delivery process, beginning with identifying and envisioning the opportunity and then proceeding into implementation (see Figure 5). If you have identified an opportunity for an IoT project, leverage this Solution Path to augment your organization's project or program delivery processes. This resource should be used in harmony with existing delivery processes. If you have not yet identified specific IoT opportunities, use the Solution Path to structure the identification of opportunities by leveraging the activities detailed in the envisioning step. The Solution Path can also be used to facilitate engagement with project management leadership to proactively address questions about IoT delivery mechanics.

Figure 5. Solution Path for Executing an IoT Initiative



Source: Gartner (October 2016)

IoT Platform Services Will Evolve and Segment

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.

> By 2020, two-thirds of companies that have adopted IoT will utilize an IoT platform suite, up from one-third today.[2]

A range of suppliers is now branding themselves as IoT platform providers. Some are doing so because they want to ride the hype associated with IoT, while others are doing so because they have some IoT platform characteristics, but no existing market taxonomy fits them well. During 2017, as the market evolves, the differences between various offerings in the IoT platform market will clarify. Specifically, Gartner expects that, during 2017:

- **The IoT cloud platform market will stratify into two classes of providers, separating IoT platform core and enhanced services.** Leaders in the infrastructure as a service (IaaS) market will leverage their offerings by extending them and branding them as IoT platforms. These services will be general-purpose in nature, following the general market philosophy for large-scale cloud service providers. We expect Amazon Web Services (AWS) and Microsoft Azure to be very dominant in this space. However, the market is wide open, and there are opportunities for aspiring IaaS and platform as a service (PaaS) providers to leverage IoT as a potential path to market leadership.
- **"Platform-plus" providers will emerge, providing services that enhance general-purpose IoT services with improved tooling, targeted intellectual property or both.** GE Predix[3] and PTC ThingWorx[4] are early adopters of this approach, having announced support for running their offerings on top of general-purpose IoT cloud platforms. For organizations that already have tooling or intellectual property that can accelerate the time to value or total value of IoT solutions, this model provides an excellent way to craft and deliver new IoT service offerings. Gartner expects a significant number of providers to enter this market segment, providing niche services that are industry-, technology- or business-problem-specific.

Planning Considerations

The choice of a platform is vital to IoT success. In 2017, organizations need to:

- Begin evaluating platform providers
- Assume a cloud-first IoT platform perspective

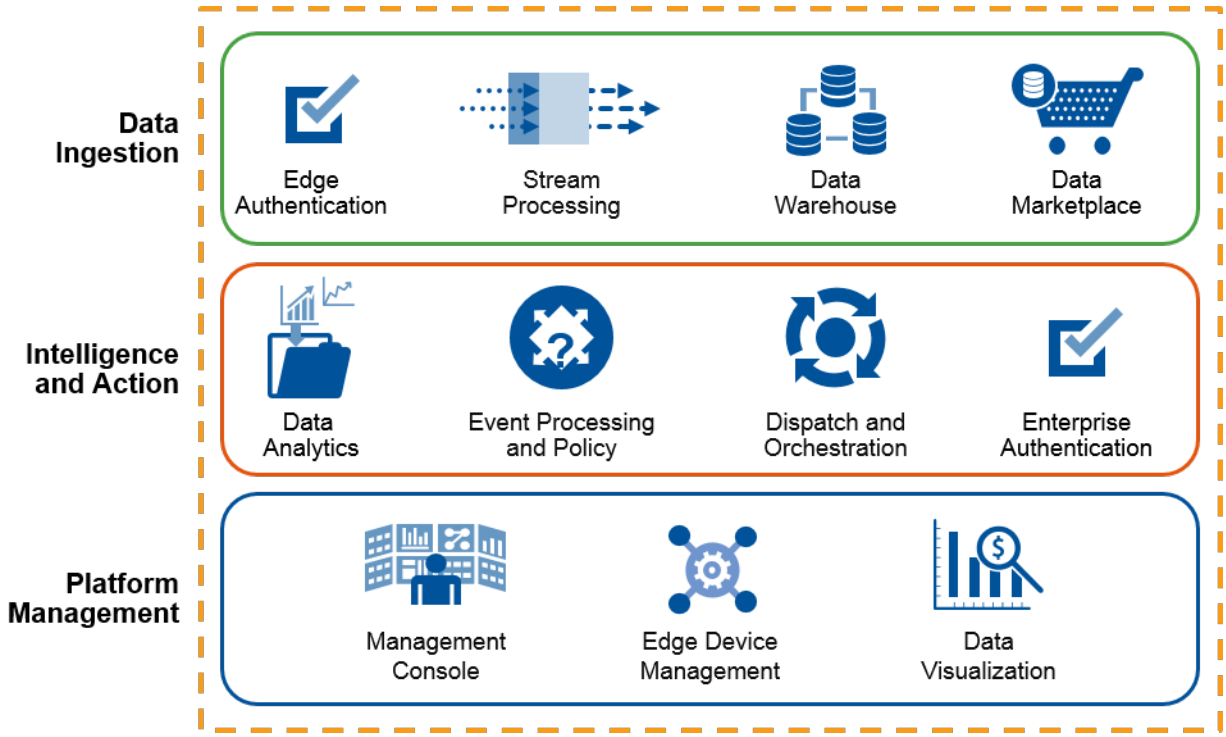
- Educate sourcing and purchasing centers about "IoT washing"

Begin Evaluating Platform Providers

Business demand for IoT will grow rapidly in 2017 and accelerate for some time. Don't wait until the organization decides to act to begin your platform evaluation process — set aside time to understand the market and the likely providers now. This undertaking does not need to be a cumbersome, formal selection process. The important priority is to come up with an appropriate shortlist of providers and to understand how they can enable your early development efforts.

The IoT platform ingests, stores and performs analytics on data and, based on the intelligence gleaned from that analysis, orchestrates tasks or invokes enterprise applications. The IoT platform also contains some device and platform management functionality. The major components are illustrated in Figure 6.

Figure 6. IoT Platform Reference Architecture



Source: Gartner (October 2016)

In 2017, technical professionals should:

- **Examine and understand IoT platform architecture.** IoT platforms are powerful enabling forces. Leverage an understanding of the architecture and key components to drive design ideas and planning in the right direction. See "Preparing, Planning and Architecting for the Internet of Things" for full details on the IoT Platform Reference Architecture depicted in Figure 6.

- **Develop a shortlist of platform providers.** Gartner explored criteria for evaluation of IoT platforms in "Exploit the Strengths of the Public Cloud for Your IoT Platform." This research will aid organizations engaged in the procurement of IoT platforms. In addition, technical professionals should leverage the 11 essential architectural components identified in the IoT Platform Reference Architecture (see Figure 6) to structure conversations with providers and to enable the early rejection of platform pretenders.
- **Include platform-plus providers in shortlist development.** These emerging providers partner with general-purpose platform providers to improve time to value, reduce total cost of operations or enable advanced solution capabilities. As technical professionals develop their shortlists of general-purpose platform providers, they should also monitor the market for platform-plus providers that could offer valuable partnerships or collaborations.

Assume a Cloud-First IoT Platform Perspective

Why favor the use of a cloud-based IoT platform for development? Key reasons include the following:

- **Cloud capabilities are the perfect fit for IoT platform requirements.** IoT solutions generate a high volume, velocity and variety of data, all while demanding stable system performance. The origins of the data are often geographically dispersed. Cloud-based IoT platforms address these issues with their geographic reach, stream-processing elasticity and data-processing capabilities. IoT solutions housed within a cloud provider can exploit all of the capabilities of the provider, including:
  - Data analytics
  - Machine learning
  - Visualization
  - Application integration
  - Service management
- **The entire platform is available immediately.** Many cloud-based IoT platforms implement all of the elements of Gartner's IoT Platform Reference Architecture. This allows for a ramp-up to basic functionality that is measured in minutes or hours, rather than weeks or months. Even if you plan to use a private or custom-built platform, leveraging a general-purpose cloud platform can enable immediate development. Given the low cost associated with these services, many organizations can get started with proofs of concept without having to request a special budget for them.
- **IoT platform costs are hard to estimate prior to the creation of a working prototype.** Many organizations discover during the prototype or pilot phase that their expectations regarding functionality and data (velocity, variety and volume) lacked clarity. In addition, organizations often discover unanticipated analytical or orchestration value during the development of IoT solutions. Metered licensing of any kind will be hard to forecast. Difficulty forecasting system

components or their usage make the licensing of IoT platform components difficult. In the cloud, there is a clear price schedule to account for increased utilization. In a customer-owned solution, however, increased utilization can trigger out-of-cycle contract negotiations — and when negotiations occur after an organization has committed to a tool, suppliers have the leverage. Open-source software is not immune to this problem because IoT can drive needs for new infrastructure, such as networking and storage.

- **Skill and technology overlaps with existing service providers can often be leveraged.** Organizations that are already using a cloud service provider will achieve faster time to value if they can leverage an IoT platform from the same provider. The architecture elements used to build IoT platforms are almost entirely leveraged from other parts of IaaS and PaaS cloud providers' offerings. This creates a significant opportunity to use common tools across multiple IT efforts.

"Exploit the Strengths of the Public Cloud for Your IoT Platform" provides a detailed analysis of the technical benefits associated with an adoption strategy for a public cloud IoT platform. In addition, because cloud IoT platforms inherit the benefits (and problems) associated with IaaS and PaaS adoption, research on the broader topic of public cloud planning will also be useful, including:

- "Solution Path for Implementing a Public Cloud Adoption Maturity Plan"
- "Building an IT Business Case for Public Cloud IaaS or PaaS"
- "How to Budget, Track and Reduce Public Cloud Spending"

Educate Sourcing and Purchasing Centers About "IoT Washing"

Suppliers and service providers have a strong desire to reposition their offerings to align with media trends. This market reality led Gartner to develop the Hype Cycle as an analytical tool. In 2017, many suppliers will engage in "IoT washing" — that is, repositioning their existing products as IoT offerings. A key challenge for technical professionals will be to engage with and alert IT, business and purchasing stakeholders to this fact, as well as to proactively identify valuable partnership opportunities. To guard against the potential downsides of vendor IoT washing, there are a few important steps to take in 2017:

- **Clearly identify a primary contact in IT for IoT.** Even if the organization is a purely digital one, or has decided to defer action on IoT, it is still important to identify an official point of contact for IoT-related issues. Most organizations embed this contact within either the CTO's organization or the enterprise architecture group, but the location on the organization chart isn't what is important. The critical priority is to have a single point of contact who can ensure that the organization isn't purchasing redundant capabilities and who can prevent buying centers from being bamboozled.
- **Watch out for services and products that are suddenly IoT-enabled.** In many situations, vendors will tout new IoT features or functions that have been added to their services or products. New capabilities are great when they provide functions that the organization cares about. Be on guard, however, against supplier attempts to use "IoT enablement" to change fee structures or to upsell.

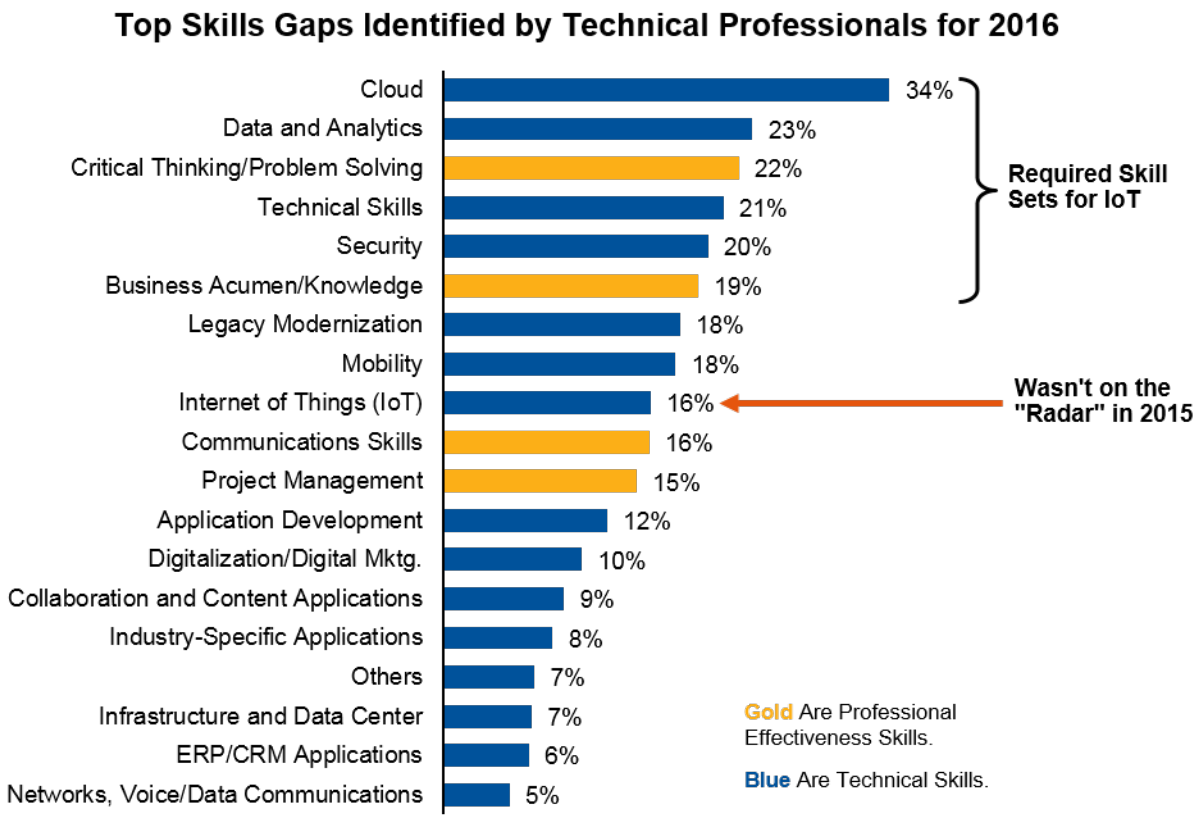
- **Beware of license restrictions on existing APIs.** Integration is essential to IoT. Because so many opportunities exist to integrate with existing edge capabilities, many suppliers will see a dramatic increase in the use of existing APIs — and these suppliers will try to monetize that utilization. To avoid paying for capabilities you may have already purchased, educate buying and sourcing groups about the hazards of existing functions becoming "features" due to new IoT-generated interest.
- **Expect an increased velocity of change within the supplier community at large.** IoT will cause shifts in a wide range of products and services that your organization consumes. IoT innovations will transform laggards into leaders, trigger mergers and drive acquisitions. Technical professionals have an opportunity to help the business understand how IoT triggers these market changes and try to benefit from them.

The IoT Architect Will Emerge as an Essential IoT Role

2017 will be the year that the IoT architect emerges. Many Gartner clients are already including IoT-specific roles in their 2017 budgets and staffing plans. The recognition of the need for IoT skills is accelerating rapidly. In 2015, only a very small number of organizations were concerned about IoT skills preparedness. By early 2016, however, 16% of organizations were concerned about IoT skills gaps in their staffing, according to a Gartner survey[5] (see Figure 7).

> In 2016, IoT skills went from "off the radar" to a concern for 16% of organizations.

Figure 7. How IoT Relates to Broad Market Skills Gaps



Source: Gartner (October 2016)

Not everyone who will provide the needed IoT skills will be an IoT architect, but IoT delivery teams will need individuals in this role. Although the specific title and organization chart location for IoT architects will vary considerably, the person who fills this role will be responsible for:

- **Engaging and collaborating with stakeholders to establish an IoT vision and define clear business objectives.** IoT creates immediate links between business activities in the physical world and back-end processes — piercing many existing time and space barriers in the business — while increasing the involvement of many non-IT groups, such as OT teams. This increased need for communication is not a one-time requirement. Rather, it will be needed on an ongoing basis for the successful operation and evolution of the IoT solution. This is not the space for "lone wolves" or individuals with a reputation for unilateral action.
- **Designing an edge-to-enterprise IoT architecture.** Many organization will pursue and operate multiple IoT solutions. This can lead to redundancies that increase operational complexity, consume time and increase costs. The IoT architect must identify and document the IoT target state for the organization as well as ensure that the target architecture will address business requirements now and in the future. Organizations can't continue to create new legacy systems. Instead, they must craft and utilize an architecture that can expand and evolve over time.

- **Establishing processes for constructing and operating IoT solutions.** Processes will be needed for IoT solution development, delivery and execution. Although heavyweight processes are not always the answer, "code and fix" approaches are never the answer. The challenge will be to "rightsize" these IoT processes to the task at hand. This is best achieved when there is a clear and collaborative partnership between individuals with technical, operational and project domain expertise. Collaborations need leadership — someone must ensure that they occur, are focused on the right outcomes and do not grow out of control. This is best accomplished by making the IoT architect the centralized point of accountability for IoT technical, operational and delivery outcomes.
- **Working with the organization's architecture and technical teams to deliver value.** IoT architects will not be able to deliver IoT solutions on their own. They will need to collaborate with a wide range of architects and technical teams across the organization — including teams that maintain infrastructure or OT that is outside the normal purview of the IT organization. In addition, many organizations will have IoT solution architects who are focused on specific business problems or on integrations with specific key components of the solution. The cross-silo penetration of IoT is not just limited to non-IT business groups. IoT also requires new collaborations within IT, and between IT and outside groups. Engagement skills are a fundamental requirement for delivering IoT — and are therefore critical skills for IoT architects.

These individuals will be hard to find. 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.

Planning Considerations

Organizations need to understand the importance of 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. In 2017, to avoid this reactive posture, IT professionals should:

- Make the case for IoT architecture and the architect needed to manage it
- Use outside-the-box thinking to fill the IoT architect role

Make the Case for IoT Architecture and the IoT Architect Role

To effectively champion the creation of the IoT architect role, you must first make the case for why IoT architecture itself is vital. IoT represents a democratization of existing technologies. The key challenge lies in organizing these technologies into new structures while removing time and distance barriers between the edge and the enterprise. Information and decisions will suddenly engage the organization more quickly and more broadly. When information and decisions are focused on the right business problems and engage the proper parties, they will deliver tremendous value. When they are not applied properly, they will cause tremendous disruption.

IoT architecture will help organizations increase the odds of successful IoT deployments by:

- **Avoiding wasted time, resources and money by centralizing coordination.** Many organizations will pursue multiple IoT initiatives, and a lack of coordination among these initiatives will likely cause waste and redundancy. The primary factor that must be addressed is talent. All of the technologies required to "bootstrap" IoT have talent demands, and organizations will need to plan for not only how they will address these talent needs, but also how they will prevent these needs from stalling other efforts. Organizations need an IoT architect to provide the coordination needed to address these issues.
- **Leveraging the portfolio of business opportunities to prioritize architecture and solution development.** Solutions can have a one-to-one relationship with problems, but architecture must have a one-to-many relationship. Architecture must also be developed and deployed in a controlled manner so that high-value functions or critical-path dependencies are deployed sooner. These types of planning and prioritization decisions cannot be made without understanding the business, as well as the sets of business problems that can be addressed with IoT. Organizations must identify a position to be accountable for collecting and managing this information, and for using it to prioritize architecture and solution development.
- **Providing the technical guidance and governance required to avoid technical debt.** Architecture should be as simple as it can be, but no simpler. Simply purchasing a product or designating a supplier as the organization's "IoT platform" or "IoT architecture" will not address redundancy and prioritization issues. Often, a single platform has multiple ways of addressing the same or similar problems. Several of the current IoT platform providers have four or more ways to store data. Just as organizations need architectural oversight of their use of other infrastructure components (such as storage, databases and development platforms), they also need oversight and planning regarding the use of all of the elements of the IoT architecture. This requires an understanding of the end-to-end architecture, the technical capabilities of the organization and the sequence of business problems to be addressed.
- **Rightsizing delivery processes based on technical and business risk.** Process is as important to successful IoT solution delivery as architecture or technology. The question of how much planning and governance are required to execute on technology projects is as old as technology itself. Whether the debates are between waterfall versus agile, Mode 1 versus Mode 2 or a 1,000-page manual versus self-documenting code, the important question isn't which choice to use. Rather, it's how to align delivery processes and governance expectations properly. Rapid prototyping has a role, but so does careful planning. If you just want to prove that something can be done, then agile, Mode 2 approaches are probably best. If, on the other hand, 20,000 devices will need to be manufactured and assembled, careful and detailed planning will be required. The key is to align the approach to the particular problem, which in turn requires an understanding of the big picture. The IoT architect plays a critical role in providing this insight and in making these choices effectively.

Use Outside-the-Box Thinking to Fill the IoT Architect Role

Ideal candidates will be hard to come by. In particular, candidates with business domain expertise will be particularly difficult to recruit because they almost always have to be poached from

competitors. Hence, creative means must often be used to help find the right candidate. Recommended approaches include:

- **Collaborate closely with HR to acquire and retain IoT architects.** Your HR department will likely have no past experience in hiring IoT architects, so it is important to invest the time needed to help them help you. Help recruiters understand the required technical and "soft skill" backgrounds. Identify and track IoT leaders at other organizations, and use them as case studies to help HR understand how to identify candidates beyond the use of simplistic keywords and checklists.
- **Include IoT architecture in 2017 talent development plans.** Meeting future talent needs is a vital function for all organizations and business units. Determine the processes used to identify, coach and mentor candidates for potential advancement, and educate process leaders about the emerging IoT architect role.
- **Understand IoT architecture to drive technical talent development.** Perform a comparison between models, such as the logical architecture for IoT solutions (see Figure 4) and the existing talent within the organization. Then focus on developing the needed technical and soft skills of the organization's existing talent. Use training and pilot projects to develop skills in areas where gaps exist. Do not rely on recruiting alone to acquire talent. IoT will create talent demands that justify the development of "bench strength."
- **Consider a center-of-excellence approach.** It just may not be practical for your organization to recruit or retain a single individual who possesses the range of technical and soft skills required. As a result, we will also see the emergence of an "IoT architecture office" or other team that leverages complementary skills from several individuals to fulfill the IoT architect function.

Security Concerns Will Continue to Be a Major Obstacle to IoT Adoption

IoT project planners need to identify and document security issues early so that remediation can be prioritized and addressed as appropriate. Failing to address security jeopardizes credibility with IoT project sponsors. The scale, complexity and operational impact of IoT elevate security concerns. Media reports of IoT security failures add to sponsor and business anxiety.

> The most expensive and disruptive strategy for any project is to ignore security issues as if they would resolve themselves. Security is most expensive when addressed as an afterthought.

IoT solutions often integrate with existing technologies and processes that are vital to the normal operation of the business. As a result, the resilience of these systems is important, and security is deeply linked with resilience. IoT failures in general have very high impact on — and therefore high visibility for — business stakeholders and customers. Organizations should be concerned with how to protect and preserve these systems.

As was the case with cloud and mobile technology, security and risk concerns are a major impediment to adoption for IoT. There have been a number of well-known and costly IoT security failures, ranging from the sabotage of the Iranian uranium enrichment program to the hacking of Jeep vehicles, that lend credence to these concerns. Both of these examples were expensive to fix, and they revealed that control systems were much more vulnerable than their designers anticipated. In the case of the Iranian centrifuge program, the equipment had been air-gapped to prevent attack code from accessing the control systems, yet the attack code was able to cross that gap. In the Jeep example, Chrysler engineers didn't anticipate the entertainment system as a usable vector to attack the vehicles' internal control bus.

> IoT solutions create new pathways into and out of control systems. "Things" that were at one time isolated from networks become attached in order to become better integrated and more powerful. Their vulnerability is also increased.

Ventilation systems, manufacturing controls and medical devices are all examples of "things" that were isolated in the past but that are now connected through IoT. In the past, attacking these systems required physical presence. Once networked into an IoT solution, they can be attacked from anywhere with internet access.

Cloud and mobile technology had to address security concerns to smooth adoption and become the success stories they are. There was a time when banks were uncertain about how to secure account holder transactions on mobile devices, but that didn't stop the rapid rise of mobile banking. By 2015, according to a recent U.S. Federal Reserve study, 43% of all mobile phone owners with a bank account were using mobile-banking services.[6]

The following are lessons from cloud and mobile that should be heeded in IoT security planning:

- **Organizations underestimate their current capabilities.** Cloud, mobile and IoT all have new aspects to them, but they are all built on foundations that are well-understood to organizations. The key to unlocking this realization is understanding and analyzing their architecture. Although some system components will take time to understand and digest, IoT security in general is not entirely new.
- **Large, diverse solutions can be deployed and maintained.** One of the issues frequently raised regarding IoT is the large number of edge endpoints and their diversity. Although IoT raises new operational and management questions that result from this complexity, mobile application development and support teams have found workable solutions — and they are able to do so on hardware and operating systems outside their direct control.
- **Shared responsibility works.** More than any other IT innovation, cloud computing requires organizations to become interdependent with outside suppliers. In the traditional data center, if the hardware supplier's business fails, the enterprise loses support but keeps on operating. If a cloud provider's business fails, however, the business faces an immediate operational issue. IoT solutions have a dual challenge in this area. Internally, they often result in the realignment of

responsibilities and tasks between IT, OT and business groups. In addition, the adoption of cloud IoT platforms creates new external dependencies.

Planning Considerations

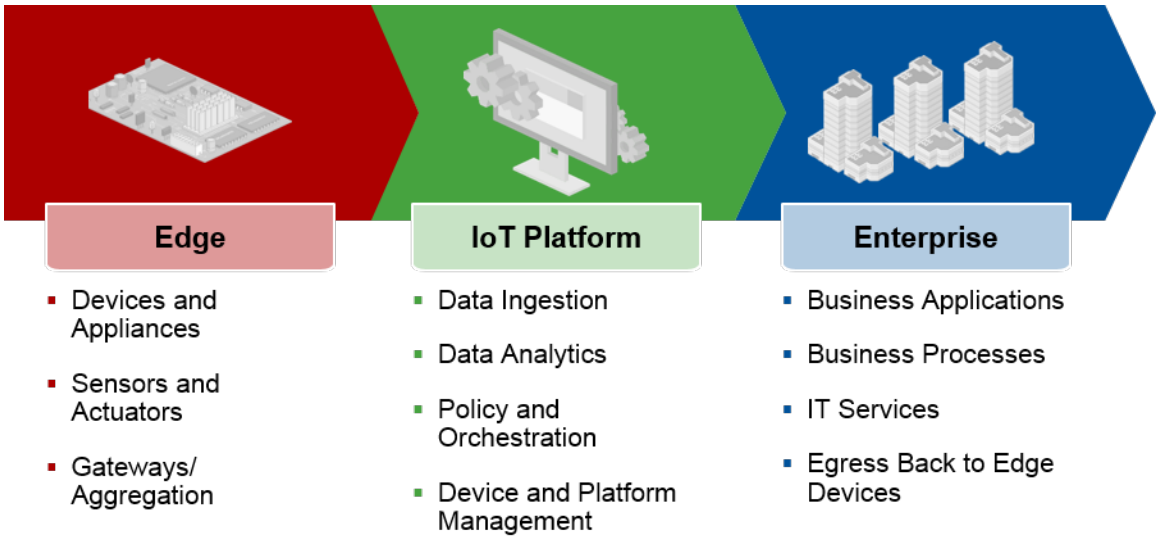
Broad questions — such as "How do we secure this?" — must be broken down systematically to be addressed. As business interest in IoT grows, technical professionals must be prepared to address such questions about IoT security. Begin such an analysis using the edge-platform-enterprise model as a starting point, diving into additional architecture details as needed.

"A Primer for Building Resilience and Security Into Internet of Things Solution Architecture" contains a deeper treatment of IoT security beyond these planning considerations.

Leverage the Edge-Platform-Enterprise Model to Structure Risk Analysis

Technical professionals should start their preparations for security and risk discussions by breaking down the architecture components. The Gartner IoT solution model shown in Figure 8 provides a good starting point by depicting the three major architectural elements of IoT solutions. (For more information, see "A Primer for Building Resilience and Security Into Internet of Things Solution Architecture.")

Figure 8. Three Parts of an IoT Solution



Source: Gartner (October 2016)

Begin by understanding IoT technical components that are either planned or in place. This will provide the architectural details that can later be cross-referenced with the privacy, safety and reliability (PSR) model (discussed in the next section) in order to provide sufficient detail for risk management and control prioritization. These technical components will fall under one of the following three major parts of an IoT solution:

- **The edge:** This is where the interaction with the physical world takes place. For most IT organizations, this is the IoT component that is the most foreign. There are three dominant concerns at the edge:

  1. *Endpoint security* — Considerations here center on managing the security characteristics of the endpoint device itself. This involves a case-by-case examination of each endpoint in an IoT system. Start by examining all of the sensors and actuation points within the solution and then identify the things they are attached to.

  2. *Communications* — Selecting a communications technology and set of protocols is often a complex decision that must balance power, bandwidth, reliability, security, cost and other concerns. A single IoT solution may include multiple communications technologies, each with its own security limitations.

  3. *Maintenance* — The final important concern at the edge involves how to understand and plan for the question "How will IoT edge devices be monitored, managed and updated?"

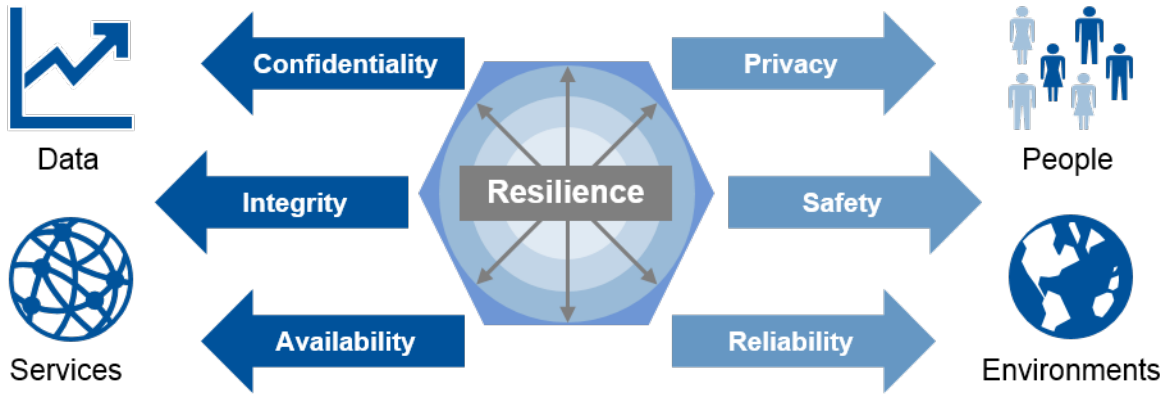
- **The IoT platform:** The IoT platform is built on top of many components that are also used to build mobile, big data and other applications (see the IoT Platform Reference Architecture shown in Figure 6). As a result, organizations can leverage their own procedures or industry best practices to secure these components. Even if a cloud-based IoT platform is the organization's first heavy investment in cloud, there is a significant amount of research — from Gartner as well as the platform providers themselves — on how best to secure these environments and their components. (For more information on IoT platforms, see "Exploit the Strengths of the Public Cloud for Your IoT Platform" and "Preparing, Planning and Architecting for the Internet of Things.")

- **The enterprise:** This is the portion of the IoT solution that your organization already has and that is already securing and maintaining. Integration between the enterprise and the IoT platform is essentially the same as integration with third-party systems, or even among internal systems. Gartner does not expect IoT to drive major changes in enterprise IT or systems control, but we do see significant business process changes. Point-of-sale devices, automobile telemetry sensors and utility meters are all examples of IoT endpoints that can be targets for fraud and deception. Often, due to cost, power or foresight constraints, technical controls are not present that can account for these risks — but analytics and business process checks can account for them instead. When evaluating risks to the enterprise or control options, be sure to include the business processes themselves.

Leverage the PSR Model to Identify Specific Risks

The PSR triad covers the environmental and people-related risks of a digital business solution (see Figure 9). 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 9. The CIA-PSR Model for Resilient IoT Solutions



Source: Gartner (October 2016)

The central element of this approach is the concept of resilience. The committee draft of International Organization for Standardization (ISO) 22316, "Societal Security — Organizational Resilience — Principles and Guidelines," defines resilience as "the outcome of an organization's capability to anticipate and respond to disruption-related risks, and its capacity to adapt to complex or changing circumstances under conditions of uncertainty." 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. A prime example is the incident in which Target's automated marketing engine figured out that a teenage girl was pregnant before her own parents knew.[7]
- **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.

Setting Priorities

Given the trends discussed in this document, Gartner recommends that technical professionals treat the following planning efforts as top priorities to ensure IoT success in 2017 and beyond:

- **Establish and maintain a portfolio of IoT business opportunities.** IoT technologies are rarely developed in isolation and then unveiled to the organization. Because they pierce time and space barriers by integrating across technical, organizational and functional silos, their planning and development require engagement and buy-in from multiple parties. Be prepared to address questions about not just why a particular IoT innovation is important, but also how this innovation was chosen and prioritized among options. A portfolio-based view of business value is required not only to drive cross-organization engagement, but also to ensure that technical and operational changes have been sequenced and prioritized to maximize time to value.
- **Leverage Gartner IoT reference architecture to identify your target IoT architecture.** IoT solutions are complex, with many integrated and interlocking elements. These elements are not of equal importance with respect to how they enable the delivery of various value propositions to the organization. Leverage Gartner research and your portfolio of business opportunities to identify high-priority architecture elements, and find ways to develop (or deepen) experience with them now.
- **Set aside time to understand IoT product and service offerings.** Cloud platform providers can contribute a tremendous amount of capability and capacity to your IoT efforts, but these products can be as complex as they are feature-rich. Use your target architecture to focus your evaluation of platform providers, as well as delivery partners that may provide implementation services or other technology components.
- **Embed IoT into skills development and recruiting.** IoT skills will be difficult to recruit — in part due to availability, and in part due to recruiters needing to develop new hunting skills. Begin to address these realities now by working with leadership to understand the skills that are needed so that the development of these skills can be prioritized — and also by working with recruiting personnel in HR to improve their ability to find and capture talent.

- **Establish IoT delivery and integration processes.** IT needs to have a plan not only for the development of greenfield IoT solutions, but also for integrating and operating IoT solutions that emerge from shadow IT, that are part of existing systems owned by the business, or that are acquired. Leverage Gartner's "Solution Path for Executing an Internet of Things Initiative" to facilitate conversations with project management, IT operations and business groups in order to engage with them and identify efficient process options.
- **Leverage the CIA-PSR model to identify risks early.** The earlier that security and risk issues are identified in design, implementation and operational processes, the less disruptive they will be to the organization and the less costly they will be to address. Build the identification of risk and security issues into the IoT culture for your organization in such a manner that identification and remediation are an ongoing process.

Gartner Recommended Reading

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

"Preparing, Planning and Architecting for the Internet of Things"

"Exploit the Strengths of the Public Cloud for Your IoT Platform"

"Assessing Integration Architecture for Internet of Things Solutions"

"Solution Path for Executing an Internet of Things Initiative"

"Leverage Intelligent Gateways in Your IoT Architecture"

"Use the IoT Platform Reference Model to Plan Your IoT Business Solutions"

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

Evidence

[1] See "Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015" and "Gartner Says Personal Worlds and the Internet of Everything Are Colliding to Create New Markets."

[2] "Use the IoT Platform Reference Model to Plan Your IoT Business Solutions."

[3] A. Hufford, "GE's Internet-of-Things Platform to Run on Microsoft's Cloud," The Wall Street Journal, 11 July 2016.

[4] "PTC Announces ThingWorx Open Platform Strategy; Integrates ThingWorx With Leading Public Device Clouds," ThingWorx, 19 April 2016.

[5] "Top Skills for IT's Future: Cloud, Analytics, Mobility and Security."

[6] "Consumers and Mobile Financial Services 2016," FederalReserve.gov, March 2016.

[7] G. Lubin, "The Incredible Story of How Target Exposed a Teen Girl's Pregnancy," Business Insider, 16 February 2012.

More on This Topic

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

- Internet of Things — Architecture Remains a Core Opportunity and Challenge: A Gartner Trend Insight Report
- 2017 Planning Guide Overview: Architecting a Digital Business With Sensing, Adapting and Scaling

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