

Unlocking value from IoT connectivity: Six considerations for choosing a provider

Companies must take a more nuanced look at connectivity providers as the Internet of Things evolves.

Kim Baroudy, Sunil Kishore, Sumesh Nair, and Mark Patel



The Internet of Things (IoT) is growing rapidly, with 127 new devices connecting to the Internet every second. Although many new applications target consumers, including smart-home systems and connected cars, others help companies optimize operations ranging from manufacturing to customer segmentation. As IoT expands, companies' connectivity expenditures will rise by about 15 percent annually through 2022. To capture this growth, connectivity providers will extend their coverage and investigate innovative technologies, including low-power, wide-area networks (LPWANs).

Such shifts could have major repercussions for companies that sell IoT devices or services. For many years, they relied on country leads to select connectivity providers, and the default choice was often the largest regional or local player. A few also asked systems integrators for provider recommendations, often with similar results. But as IoT becomes more important to the bottom line, companies must reassess their connectivity needs and make more nuanced decisions that consider global coverage, intelligent-switching capabilities, service delivery, pricing, security, and IoT expertise.

Global coverage under one contract

For mobile connectivity, companies often have multiple country-specific contracts, all with different terms, pricing, and coverage options. With IoT, a simpler path may make more sense: having a contract with one mobile network operator (MNO) or mobile virtual network operator (MVNO) that provides global connectivity through a single platform. To ensure coverage beyond its established base, the selected connectivity provider must tap into its roaming agreements with other MNOs or MVNOs or seek new partners to fill gaps.

The single-contract approach helps companies minimize complexity, since responsibility for global coverage falls to the provider, rather than to the company supplying IoT devices or services.

Using one MNO or MVNO also gives companies more insight into their data usage because they can monitor it through a single platform.

Strong intelligent-switching capabilities

Many providers are investigating two intelligent-switching technologies, both of which are relatively new. The first, intelligent mobile switching, enables IoT devices to shift seamlessly from one MNO or MVNO to another. It is still uncommon for IoT devices to have this ability. The second technology, intelligent platform switching, lets devices transition among unlicensed, cellular, and mobile platforms depending on their data-transmission requirements and other factors. No IoT devices are yet capable of platform switching, but some companies are increasing their investment in this area.

Mobile switching can take various forms. Some IoT players enable this capability through multiple international mobile subscriber identity (multi-IMSI) technology, which allows a single subscriber-identity module (SIM) card to be assigned numerous local numbers, including those for different countries (Exhibit 1). This tactic keeps roaming charges lower than those obtained through bilateral agreements with other providers. Since multi-IMSI networks are still not widely available, most companies cannot take advantage of them and still incur roaming charges.

Embedded universal integrated-circuit cards (eUICCs), an emerging SIM technology, may eventually represent a better solution than multi-IMSI for mobile switching in IoT. Each eUICC hosts profiles of multiple MNOs that users can remotely add or remove on demand, potentially giving them more control over roaming costs and quality than multi-IMSI technology.

Few MNOs and MVNOs now provide eUICCs, partly because the technology is so new, but customers may begin to request this option as they learn more about

its value. If eUICCs become mainstream, they could become the default connectivity option—lowering costs dramatically and potentially disrupting the industry. But enterprises must carefully evaluate the benefits and trade-offs of eUICCs before aggressively pursuing this option. For example, eUICCs are a relatively immature technology and thus may raise a host of reliability issues or customer-experience problems. Enterprises also risk losing subsidies or discounts from MNOs if they move to eUICCs, or they may find that their eUICC provider does not connect to all the MNOs needed to achieve their coverage goals.

Strong service-delivery capabilities

With mobile connectivity, companies naturally favor providers with good track records for quality service because outages will result in a barrage of customer complaints. But most fail to apply the same logic when evaluating their IoT connectivity needs. With IoT devices just beginning to gain traction, an outage may seem like a minor problem compared to the chaos that occurs when mobile users lose cellular coverage. This misconception may cause procurement leads to downplay service quality

and focus on cost issues when selecting an IoT connectivity solution. In such cases, the vendor of choice is often a company’s current mobile provider or the least expensive alternative.

Although cost issues deserve attention, companies will soon recognize that poor service could derail their fledgling IoT offerings. For instance, drivers of connected cars that lose online navigation capabilities in remote regions are likely to assign blame to the business that sold the IoT device, rather than the connectivity provider. As companies begin to place more weight on service quality, they should focus on the following provider characteristics:

- **Leadership and strategy.** The best IoT connectivity providers are committed to innovation and invest in the latest technologies, including eUICCs.
- **Specialized knowledge.** Companies should favor connectivity providers that truly understand their industries and offer tailored products and services for each customer, rather than a suite of generic offerings.

Exhibit 1 Two competing subscriber-identity module (SIM) technologies could enable intelligent network switching.

Multi-international mobile subscriber identity (multi-IMSI)



Multiple international operator profiles preloaded into single multi-IMSI SIM mount

Embedded universal integrated-circuit card (eUICC)/reprogrammable SIM



Operator profiles can be remotely added or removed from eUICC on demand based on user needs

- Customized plans and performance measures. Standard service-level agreements (SLAs) often leave much to be desired. For instance, they might state that providers must restore connectivity after an outage but not specify the time frame when this must occur. A better option involves asking for customized contracts with specific key performance indicators (KPIs). In the case of service disruption, the contract could reflect the customer’s desired deadline for service restoration—say within three days—and have KPIs that track the percent of outages extending beyond that time. Or if a company wanted to improve its call-center service, the contract could specify that providers must answer 90 percent of service calls within 45 seconds and limit hold times to three minutes in 80 percent of cases.
- Risk management. The danger of a catastrophic event looms over every business, and for IoT that could mean a widespread outage affecting thousands of devices. Contracts should reflect such dangers by including risk-management and contingency plans.

Customized pricing

Most IoT connectivity providers offer multiple pricing plans with different data limits and other features—one plan might have low set-up fees and high overage charges while a second offers the opposite. When evaluating their options, most companies choose a standard plan, rather than requesting a customized offering, because they lack insight into their connectivity needs and usage patterns. Without this information, they often pay for unnecessary features, such as a data-volume allowance that far exceeds their requirements.

The creation of a customized pricing plan may seem daunting, but a simple approach can help. As a first step, companies should determine how employees are using IoT devices within their organization, as

well as how customers are using their IoT-enabled products. During this analysis, they should focus on their most important use cases, which can relate to internal operations, customer needs, or both. Companies can then classify their organization into one of three categories based on data needs (low, medium, or high). Roaming and connectivity requirements, as well as the need for overage protection, may vary within each of these categories, as shown in Exhibit 2.

Let’s consider the example of a logistics company, identical to the one discussed in the exhibit, to understand the factors that dictate its contract requirements. This company operates a fleet of 1,000 trucks across Europe in a seasonal industry. The trucks tend to make local trips over the same routes rather than long journeys that span countries, and they have low data requirements. Since this profile would put the company in category one, it would likely prefer a package that charges for limited data volume. The company would also want both satellite and mobile connectivity (meeting needs for both land and sea, since some trucks may have to be transported by ship on rare occasions). Data usage might vary by truck, with some using much more than others, so a contract that includes a pooled data plan would be preferable. Providers might also win the company’s business through more flexible pricing options. One draw might be a plan that allows the client to carry unused data forward, since business varies by season.

Emphasis on security

As IoT implementation increases, so will threats from hackers. When companies are trying to determine how well connectivity providers can combat such intrusions, they should focus on three areas: infrastructure, endpoint security, and encryption techniques.

Infrastructure

Most providers offer strong network-design

Exhibit 2 Enterprises can be divided into three broad categories based on their data requirements.

	Category 1: Low data usage	Category 2: Moderate data usage	Category 3: High data usage
Example use case	Pan-European logistics company operating fleet of 1,000 industrial trucks	Healthcare company in North America providing clinical remote monitoring for 1,000 devices	European municipality with standard smart-city road and traffic-management system involving 1,000 devices
Data volume	20 GB/month	200 GB/month	400 GB/month
Connectivity type	Satellite and cellular	Cellular	Wi-Fi and cellular
Contract features			
Data-plan requirements	Pooled data plan, since data utilization varies by truck and data volume can be shared among devices	Tiered data bundles required, since devices have different data-monitoring requirements	Standard data bundles are the best option, since each device has regular data-usage patterns
International and roaming	Pan-European bundles: Company benefits by negotiating set international rates and bundles across European network operators, which minimizes roaming costs	International roaming: Company negotiates set rates with global network operators to minimize roaming costs for the small number of users who travel internationally	Domestic data plans: Company selects this option because it does not require an international data plan
Overage and other charges	Data carry-forwards: Unused data can be carried forward, which is helpful for a business with seasonal variations	High overage charges: Low volatility in data usage allows the company to accept higher overage charges in exchange for lower base rates	High overage charges: Low volatility in data usage allows the company to accept higher overage charges in exchange for lower base rates

measures and process-design protection, including traffic separation and access management, but there may be important differentiators related to technology-design protection, including firewalls. Companies should also gauge how quickly providers can respond to hacker intrusions.

Endpoint security

Most IoT players are reluctant to require device

authentication, a process in which a machine's credentials are compared to those on an authorized list to determine if it has permission to access the system. But the cybersecurity threats to IoT may require them to reconsider this stance. For instance, they might decide to ask device users to enter passwords before connecting a device to IoT, and would thus need providers who can support this capability. IoT device manufacturers

must also fortify their systems through signature detection (determining that a device is infected and communicating with hackers) or by looking for traffic anomalies. The ability to spot traffic aberrations in real time could give providers a great advantage.

Encryption standards

Cryptography—the process of transforming plain text into encrypted text—is essential to protecting the integrity of data transmitted over IoT and keeping them confidential. But companies should keep in mind that all encryption processes are not created equal when evaluating providers. For example, they should seek providers with encryption methods that allow for agility—in other words, those with base algorithms that can easily adapt and evolve in response to an attack. In addition, companies should ensure that providers follow best practices for cryptography. Consider issues related to crypto keys—the algorithms that encrypt text. If a provider uses a system-wide crypto key, hackers that unlock the code could breach its entire organization.

While many connectivity providers are strong in one or two of these areas, few offer comprehensive security solutions that incorporate all three defenses. Unless they step up their game, IoT players will need to contact cybersecurity specialists for additional protection.

IoT connectivity expertise

As IoT connectivity requirements increase in complexity, and as options continue to multiply, companies will need providers who can advise them about the best solutions and potential partnerships. These providers may include both start-ups specializing in IoT and established players in the mobile sphere.

As discussed, companies appreciate contracts that include tailored pricing based on data usage

and roaming. But the best providers will take customization beyond that by looking at each customer's top use cases and considering their specific requirements—for instance, the typical frequency of data transfer and reliability needs. With this information, they can identify the best connectivity solutions.

Consider, for instance, requirements within the connected-car sector, where one company could offer multiple IoT applications, including those for fleet management, in-vehicle entertainment, and stolen-vehicle recovery (Exhibit 3). Each use case has different data requirements for rates, frequency of transfer, and data per report. However, all use cases require the same degree of reliability, security, and coverage. By contrast, industrial and retail applications often have strikingly different data requirements, as well as varying needs for coverage, reliability, and security.

To determine the best connectivity solution, companies must identify their top one or two use cases. (In some cases, the top use cases may relate to IoT applications used internally, rather than those used by customers.) They should then work with providers to identify optimal connectivity solutions and develop tailored contracts.

Companies will also appreciate providers that can advise them on the best connectivity technologies. Some IoT players, for instance, will soon need to find alternatives to 3G networks because these are being discontinued in their areas. Others might want to investigate LPWANs. Although these networks now cover only 20 percent of the global population, this may increase to 100 percent by 2022. As their name implies, LPWANs allow long-range communications among connected devices while optimizing both costs and power-consumption requirements. Despite these benefits, the move to LPWANs is not always advisable because they do not provide

Exhibit 3 Best-in-class IoT connectivity providers can build customized IoT connectivity solutions for specific use cases.

Data requirements for Internet of Things (IoT) applications

● Low ● Medium ● High

	Application (select examples)	Data rate	Frequency of data transfer	Data per report	Traffic (MB/device/month)	Reliability requirements	Security	Level of coverage
 <p>Connected-car applications</p>	Fleet management	Medium	Medium	Medium	Low	High	Medium	Global
	Usage-based insurance	Medium	Low	Low	Medium	High	Medium	Global
	Stolen-vehicle recovery	Low	Low	Low	Low	High	Medium	Global
	Vehicle platform	High	High	High	High	High	Medium	Global
	In-vehicle entertainment and access	High	High	High	High	High	Medium	Global
	Vehicle diagnostics	Medium	Low	Low	Medium	High	Medium	Global
 <p>Connected-industry and -retail applications</p>	Retail-goods monitoring and payment	Medium	High	Low	High	High	High	National
	Agriculture yield	Low	Medium	Low	Low	Medium	Low	National
	Public-space advertising	Medium	Medium	Medium	Medium	Medium	Low	National
	Manufacturing and processing	Medium	Medium	Medium	Low	High	Medium	National
	Logistics routing	Medium	Medium	Medium	Medium	High	High	Global
	Predictive maintenance, including equipment	Medium	Low	Low	Medium	High	High	Global
	Vending machines	Low	Low	Low	Low	Low	Low	National

Source: 4G Americas; expert and customer interviews; McKinsey analysis

the most reliable coverage. Enterprises might not understand such nuances, but a knowledgeable provider would.



Both new and established connectivity providers are aggressively trying to win business in the IoT sphere.

Their proliferation, combined with the emergence of new technologies, creates more connectivity options than ever. While companies may be tempted to focus on cost, as they have done for many years, the best players will take a more thoughtful approach by developing a detailed understanding of their connectivity needs—often for the first time—and then seeking providers who combine top capabilities

with tailored solutions. With the right connectivity provider, companies will be able to take IoT to a new level—and their bottom line will reflect the results. ■

Kim Baroudy is a senior partner in McKinsey's Copenhagen office, **Sunil Kishore** is a partner in the Atlanta office, **Sumesh Nair** is an associate partner in the London office, and **Mark Patel** is a partner in the San Francisco office.

Copyright © 2018 McKinsey & Company.
All rights reserved.