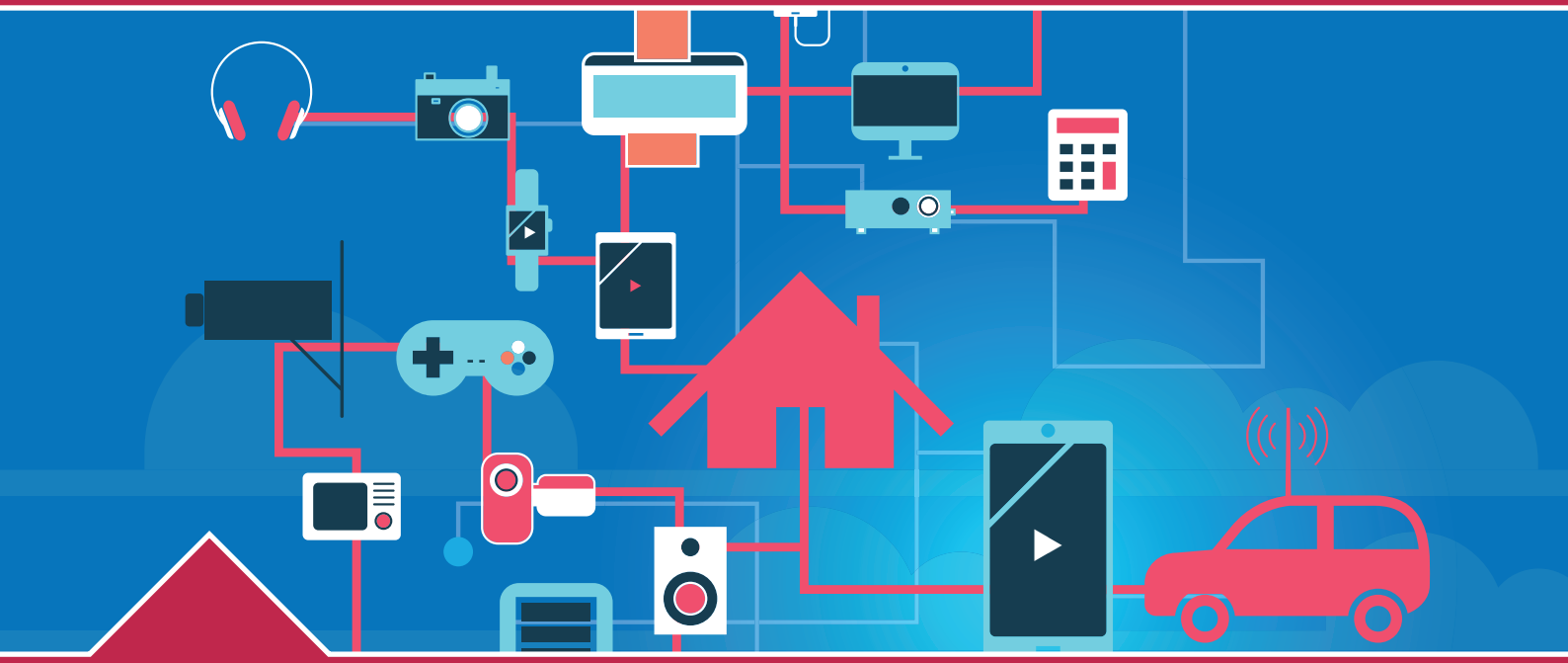
telecoms.com INTELLIGENCE



IoT Outlook 2015

Contents

Welcome

Welcome to the IoT Outlook 2015, a dedicated report by Telecoms.com Intelligence investigating the future of the Internet of Things.

IoT promises to change how society operates in the years ahead of us. With intelligent machine-based communications, our industry is at the start of a very long journey, and the end goal currently remains undefined.

Operators can expect to be firmly planted in the middle of the connected world of the future; simultaneously managing the data and traffic requirements from consumer, enterprise, industrial and governmental sectors. Not only will the operator network have to prioritise traffic when necessary, such as smart city or critical communications-related data, but it will also have to do so securely, flexibly and automatically, with the intelligence to analyse data in real-time.

With hundreds or thousands of different use-case scenarios possible for M2M and IoT, the telecommunications sector can be expected to act as the glue holding the entire industry together. Cellular networks will evolve towards 5G over the next five to ten years, and early research efforts into this almost ethereal technology have focussed on IoT capabilities as a primary requirement for its development.

There's so much expectation surrounding IoT, and so much industry buzz, that it can appear overwhelming even finding the right place to start, much like trying jump on board a speeding train. The industry is gathering momentum at a startling pace and today's culture of on-demand, instant gratification means we're clamouring for an IoT world before we're capable of creating it.

This survey, conducted by Telecoms.com Intelligence gathered the viewpoints and opinions of nearly 1,000 telecoms and enterprise technology professionals, all of whom have their fingers firmly on the pulse of the industry. We then undertook extensive analysis to identify the main trends we're observing today, and tried to put together the many pieces of this IoT jigsaw puzzle.

In this report you'll find dedicated sections relating to information security, network-specific challenges, cloud and big data considerations and industrial IoT applications; all starting with a broad overview of the industry as we see it today.

I hope that you enjoy the report, and that it aids you in your decision-making process as we begin this IoT adventure together.

Tim Skinner
Intelligence Content Manager
Telecoms.com

IoT LANDSCAPE

Key takeaways:

- 51.8% of respondents primarily associate the Internet of Things with consumer technology, such as home automation and wearable tech.
- 42.4% believe security challenges represent the biggest inhibitor to IoT.
- A further 37.2% see platform standardisation issues as the biggest challenge.
- 62.4% of respondents believe they'll be ready to monetise IoT by 2020.

About Gemalto:
Gemalto (Euronext NL0000400653 GTO) is the world leader in digital security, with 2014 annual revenues of €2.5 billion and blue-chip customers in over 180 countries.

Gemalto helps people trust one another in an increasingly connected digital world. Billions of people want better lifestyles, smarter living environments, and the freedom to communicate, shop, travel, bank, entertain and work – anytime, everywhere – in ways that are enjoyable and safe. In this fast moving mobile and digital environment, we enable companies and administrations to offer a wide range of trusted and convenient services by securing financial transactions, mobile services, public and private clouds, eHealthcare systems, access to eGovernment services, the Internet and internet-of-things and transport ticketing systems.

Gemalto's unique technology portfolio - from advanced cryptographic software embedded in a variety of familiar objects, to highly robust and scalable back-office platforms for authentication, encryption and digital credential management - is delivered by our world-class service teams. Our 14,000 employees operate out of 99 offices, 34 personalization and data centers, and 24 research and software development centers located in 46 countries.

For more information visit www.gemalto.com, www.justaskgemalto.com, blog.gemalto.com, or follow @gemalto on Twitter.

Connecting **things**

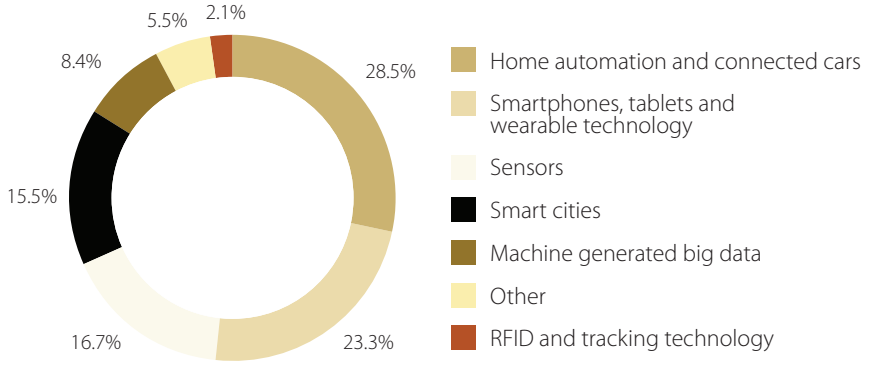
Welcome to the 2015 IoT Outlook Report, researched and produced by Telecoms.com Intelligence. This unique report will provide in-depth insight into how the telecoms industry will stand to gain as the Internet of Things reaches maturity. Close to 1,000 professionals responded to the survey, with responses coming from a broad cross-section of the industry, from operators to academics, consultants, cloud service providers, chipset manufacturers and many others.

The Internet of Things has become one of the market's hottest trends. Use case-scenarios have begun developing and the incredibly broad applicability of a very loosely-defined term has meant various industries are viewing IoT both as a huge opportunity, while simultaneously shrouded in mystery.

This survey will aim to develop granular insight and analysis covering four specific areas of IoT, including industrial applications of IoT, cellular networking challenges, network security and the use of cloud computing as an enabler for the Internet of Things. We'll give an overview of the existing marketplace to begin the report.

IoT is one of those terms that appears to have been around forever, although clarity on what the term actually means remains a point of contention. Mainstream news coverage of IoT will have one believe it's all about having one's toaster talk to one's coffee machine and designing an automated fridge that can tell one's preferred supermarket to order more eggs. But the implications of IoT will undoubtedly stretch far beyond the domestic applications of machine to machine communications, that much is sure, and because of this mass-market misconception about its applicability we began the survey by asking our respondents what they primarily associate with IoT.

Of over 900 respondents, 28.5% primarily associate home automation and connected cars with IoT, which corroborates the picture painted by broader technology media. A further 23.3% of respondents see smartphones, tablets and wearable technology as the principal aspect of IoT they identify with. 16.7% opted for sensors, the less glamorous yet likely more pervasive use-case for much of the Internet of Things.



Which of the following do you primarily associate with the Internet of Things?

Sensors, in this case, would be tiny microprocessors used to communicate even tinier amounts of data across the internet, i.e. bytes or kilobytes. Use-cases of sensors are staggeringly broad and they have the ability to transmit data about practically anything. Sensors are already in place across the world in numerous industry verticals, and as IoT expands globally the applicability of sensors appears to be one of the flagship use-cases for IoT today.

Going back to the initial survey question, 15.5% of respondents primarily associate smart cities with IoT, 8.4% reckon it's machine generated big data, and just 2.1% see RFID and tracking technology as the primary IoT use-case.

When asked which two industry segments were likely to become the most lucrative for operators in the future, respondents primarily identified Industrial IoT and Home Automation as those with the most revenue generating potential with 47.2% and 37.1% of votes respectively. Elsewhere, smartphones and tablets, connected cars and enterprise verticals gained 31.5%, 30.6% and 28.7% respectively, with wearable technology gaining 23.3% of responses. While opinion may be split on several applications, it appears that Industrial IoT is viewed as the most lucrative by the majority of respondents. Curiously, this appears to contradict the conception of IoT being a primarily consumer-focussed tech by the responses to the previous question.

We asked respondents to identify which services will be the most lucrative in the next 12 months, instead of long-term. The results from this question corroborated the feedback received previously, with Industrial IoT, smart energy and smart home picking up 50.2%, 36.8% and 34.2% of responses respectively.

We then looked to understand how IoT revenues will contribute to overall revenue in the next year. Unsurprisingly perhaps, the majority of respondents opted for the low percentiles, with 59% saying less than 10% of total revenue, and 25.4% saying 10-30%. 9% of respondents said up to 50%, with only 6.7% saying more than 50% of their revenues will be directly attributable to IoT.

One of the questions surrounding the development of a more mature IoT relates to connectivity platforms. A variety of protocols offering low-power consumption and high-efficiency data transmission are available to sensors, devices and systems; and with choice comes inevitable confusion. The Bluetooth SIG has developed a low-energy form of the protocol for M2M communication, while ZigBee has grown from its inception in 1998 as an alternative for short-range data transmission under the wing of the IEEE.

Respondents to the survey seemed unsure of these two protocols when asked to identify which two connectivity protocols will have the biggest impact on the acceleration of IoT. 16.9% chose Bluetooth Low Energy, while just 5.8% plumbed for ZigBee, which appears to indicate a lack in faith in its potential. The most popular short-range connectivity platform is wifi, with 52.5% of the audience voting it one of the two most important forms of connectivity for IoT.

In the WAN, meanwhile, rival open collaboration groups have emerged to bring forward networking topologies capable of handling widely-dispersed M2M and IoT traffic. LoRA, SigFox and Weightless-N would be primary examples. 23.3% of survey respondents reckon low-power WAN and license free spectrum will be one of the primary accelerators of IoT.

The vast majority of respondents, however, believe the cellular network, encompassing 2G through to 5G, will be the single most important form of connectivity in enabling the Internet of Things; generating 82.3% of the votes.

52.5%

The most popular short-range connectivity platform is wifi, with 52.5% of the audience voting it one of the two most important forms of connectivity for IoT.

Respondents were asked to indicate their agreement with some statements relating to the service provider and IoT on a scale of one to five, with one being total agreement and five being total disagreement. 59.7% of respondents agreed that IoT isn't at all possible without the telecoms service provider; while 50.3% of respondents disagreed with the statement "only when 5G becomes a reality will IoT flourish".

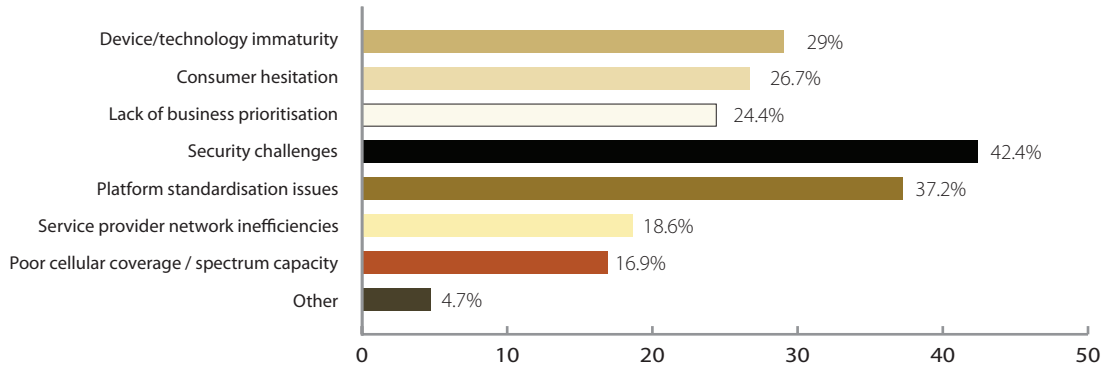
Considering the overwhelming verdict delivered on IoT-enabling platforms, perhaps it is unsurprising that the telecommunications operator was identified by 32% of respondents as being in the best position to monetise IoT. 17.5% of respondents reckon Cloud service providers are best positioned, which may come down to the necessity of having data managed and stored in an agile and always-available environment.

Most surprising, however, is the lack of consideration respondents gave to microprocessor and component manufacturers; only 6.9% of respondents believing they are best positioned to exploit IoT. If IoT reaches its full potential, industries will likely rely upon countless microprocessors that enable each sensor, device or chipset.

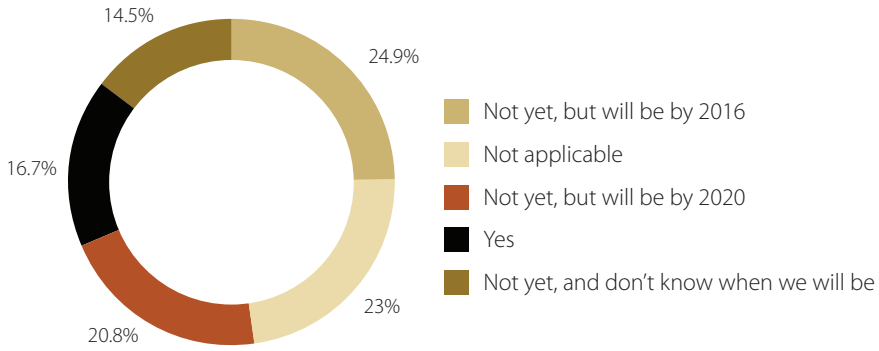
Despite its undoubted potential, considerable challenges remain which threaten the development of the IoT revolution. To that extent, we asked our audience to identify the two biggest inhibitors to IoT's development, and while opinion was spread evenly among a number of areas, two options emerged ahead of the rest.

With 37.2% of the votes, respondents identified issues relating to platform standardisation as one of the biggest challenges the industry needs to resolve before IoT can truly flourish. While various vendors position themselves around IoT, compatibility issues will inevitably arise between conflicting platforms operating across multiple devices and networks.

Some of the major challenges facing the IoT industry worthy of honourable mentions include concerns around technology



What do you consider to be the two biggest inhibitors to the IoT's development?



As a service provider, do you feel you're ready to monetise IoT?

and device immaturity (29%), consumer hesitation and trust (26.7%) and other business priorities (24.4%). What's good for the telecoms industry to see is that the two areas of least concern as identified by respondents are service provider network inefficiencies, and poor cellular coverage or spectrum capacity (18.6% and 16.9% respectively).

The biggest concern identified by participants in the survey came down to security challenges, which may offer little surprise to some readers. 42.4% of respondents agreed it was one of the two main challenges.

Since IoT emerged, security has been the biggest threat to its development and wider acceptance by the community. Some reports published in the mainstream media have hyperbolised the hidden threat posed by the IoT to personal data, particularly when we consider the connected home and smart devices. As a consequence, it's imperative that the IoT stack is comprehensively secured at every level; from device hardware and software, to the network gateway and connectivity protocols to the WAN, service provider or cloud network. To gain trust among consumers and enterprise customers alike, the infrastructure behind the Internet of Things requires a collaborative and comprehensive approach to IoT security.

We asked the audience to state its level of agreement with a few statements relating to security in the IoT stack. As expected, statements about the importance of security gained a high level of agreement. 77.1% of respondents agreed that security needs to be assessed very carefully and to ensure security of what matters, when and where it matters. Meanwhile, 69.7% of respondents agreed that trust is essential to the future of IoT development, and that it's required to ensure mass market acceptance of the technology.

In what may be considered a sizeable concern, 22.4% of respondents agreed that they do not know how to secure their IoT applications, nor do they know where weak links are prominent, with a further 12.9% indicating total agreement. Interestingly, 53.5% agree that security is an afterthought for vendors designing IoT solutions; so it appears respondents believe the vendor community remains culpable for building in IoT security at the product development stage.

Considering the variety of responses received relating to the challenges associated with IoT, and that 35.3% of respondents aren't in a position to ensure IoT security, it is not surprising then to see that just 16.7% of respondents believe they are ready to monetise IoT services today. 24.9% concede they are not yet ready to do so, but will be by 2016, with a further 20.8% believing they will be by 2020. While 23% of respondents stated the question was not applicable to their organisation type, 14.5% of respondents stated they're not yet ready to monetise IoT, and that they also can't be sure on when they will be ready.

The Elysium of a monetised Internet of Things industry is certainly edging closer, and 2020 appears to be realistic as a target date for exploiting its monetary potential. There remain a number of challenges along the way, and this report will attempt to provide you with some useful insight and guidance in your IoT journey.

Sponsor Comment

The Internet of Things has been one of the most talked about subjects in recent times, whether at technology events, on social media or even in casual business meetings. Mobile network operators, cloud enablers, OEMs, data scientists, digital security specialists or technology evangelists – everyone is contributing to the hype of this new phenomenon, along with trying to establish their role as its key enabler. The data scientists suggest that IoT would be impossible to implement without big data. Device or module manufacturers and cloud enablers argue that it's the technological advancements in their fields that have been the key impetus to the evolution of IoT. The reality is that any use case of IoT is an amalgamation of many different players in the ecosystem, the relative importance of each varying greatly from one use case to the other. While it might be too early to predict which player would eventually contribute the most to this value chain or benefit the most from it, there are various attempts in the industry to identify the key underpinnings of this ecosystem – this survey being one such attempt.

With a strong track record of implementing complex digital ecosystems, Gemalto can safely envision one pivotal factor that would govern the success of any IoT ecosystem: trust. No amount of investment in sophisticated technology or services can produce results if people, the eventual beneficiaries of the internet of things, do not trust the underlying system of networked things. Trust that the hardware, the software and the data will deliver on its promise of a connected lifestyle that is both convenient and safe. We are pleased that the respondents of this survey concur. Telecoms.com has a very knowledgeable base of followers, so we really value the results of this survey. Not surprisingly, the respondents are very conscious about the importance of security and standardization, both extremely important for building trusted ecosystems. We hope that you will find the results of this survey quite insightful in shaping your strategy for a connected world.

Happy reading.

INFORMATION SECURITY

Key takeaways:

- 42.2% of respondents believe InfoSec is the biggest inhibitor to the development at IoT.
- 44.7% say between 10%-40% of IoT data will be considered "sensitive".
- 44.8% reckon wifi is the most challenging technology to secure .

About F5:

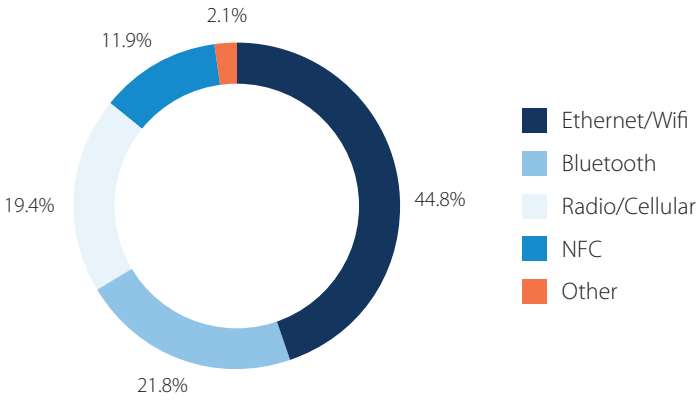
F5 (NASDAQ: FFIV) provides solutions for an application world. F5 helps organisations seamlessly scale cloud, data center, and software defined networking (SDN) deployments to successfully deliver applications to anyone, anywhere, at any time. F5 solutions broaden the reach of IT through an open, extensible framework and a rich partner ecosystem of leading technology and data center orchestration vendors. This approach lets customers pursue the infrastructure model that best fits their needs over time. The world's largest businesses, service providers, government entities, and consumer brands rely on F5 to stay ahead of cloud, security, and mobility trends.

For more information, go to f5.com.

Network insecurities

Highlighted earlier on in the report, the security of Internet of Things-based devices and networks is the most commonly agreed upon challenge cited by our audience. Of just under 1,000 respondents, 42.4% reckon the single biggest inhibitor to the development of IoT, and consequently the broad-scale adoption of the technology as a revenue generator for telecoms operators, is security.

This section of the report will look to understand the primary concerns surrounding IoT security, and provide insight as to how operators may look to mitigate the information security risk presented to the operator network and to user/enterprise privacy.



Which form of device connectivity do you feel is most challenging to secure?

Feeling a little sensitive?

We began this part of the survey by asking respondents to identify how much IoT data will contain sensitive information. The majority of responses, 44.7%, reckon between 10% and 40% of IoT data will be considered 'sensitive', with 33.8% of respondents suggesting sensitive information could be carried by anything upwards of 40% of IoT data.

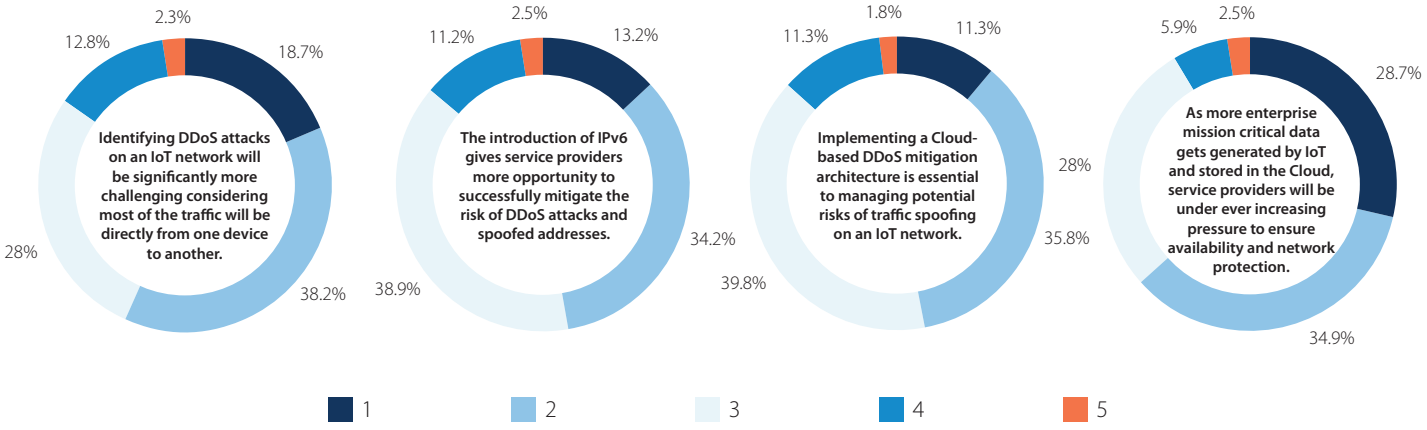
It would be worth noting, however, that the definition of "sensitive" could vary wildly depending on which of the distinct mini-ecosystems in existence within the broader Internet of Things. The definition of the word from a consumer/smart-home perspective would encompass personally identifiable information and little more, with the exception of finance or banking details. However, the likelihood of domestic appliances or systems carrying anything other than anonymised commands is minimal. In an enterprise vertical environment, M2M communications are more likely to contain information relating to company procedures, policies or even more sensitive collateral which execs would want to keep out of prying hands for financial and PR reasons; particularly if said data contains information on the company's customer or employee-base. Sufficient stories pertaining to personal and corporate hacking efforts have broken in the past couple of years, followed by substantially negative PR, not to mention regulatory fines.

Considering the domestic angle, though, and the same would be applicable for corporate networks, the device or sensor isn't necessarily the greatest risk in and of itself. What each "thing" or "machine" could be seen to represent is a single point of entry to the wider network, where more sensitive or personally identifiable information could be accessed by evil-doers.

To that extent, we then asked our respondents which form of device connectivity will be the most challenging to secure in an IoT environment. The security challenge most frequently identified by our audience, with 44.8%, was wifi; the reason for this, perhaps, is due to the huge variety of device types gaining access to a domestic or enterprise network. Despite the WPA2 security protocols existing for personal and enterprise-grade routers, the skill of wifi hacking is becoming increasingly easy to acquire for beginners.

44.7%

The majority of responses, 44.7%, reckon between 10% and 40% of IoT data will be considered 'sensitive', with 33.8% of respondents suggesting sensitive information could be carried by anything upwards of 40% of IoT data.



On a scale of one to five (with 1 being strongly agree and 5 being strongly disagree), please indicate your agreement with the following statements regarding DDoS.

Our audience was then asked to identify which two parts of the service provider network are the most vulnerable to interception or attacks in an IoT environment; and, while 36.6% of respondents identified the gateway as most vulnerable, 52.7% voted for cloud-based applications and services. A further 46.4% chose the Access network as the most vulnerable point, while the data centre, RAN, backhaul and network core received 25%, 18.5%, 11.2% and 9.7% of votes respectively.

Having highlighted potential risks to the service provider network in varying forms of technology and protocol, ranging from wifi and Ethernet down to the network's core; the security challenges facing the telecoms industry ahead of a more expansive IoT push is considerable. Opinion, however, appears divided on what exactly poses the most obvious threat. What did appear a point of mutual agreement, though, is that 62.9% of respondents agreed with the statement "service providers will have to significantly increase security investment to sufficiently protect the IoT", which should play as music to the ears of information security vendors who are armed with a suite of IoT-ready InfoSec solutions. And while 31.4% of respondents actively disagreed with a statement implying the IoT will be impossible to fully secure due to the variety of technologies involved with it; a further 62% of the audience did agree that real-time analytics of IoT data will be essential to detecting and mitigating security risks.

Such risks could well present themselves in the form of distributed denial of service (DDOS), which manifests itself as a targeted and concerted effort by attackers to overload a network with spoofed traffic, to grind it to a halt and provide a significant distraction for further exploits. Smart devices, in essence, could be considered as DDoS attack sources.

Is M2M DDoS harder to detect?

In an IoT environment where traffic generally flows directly between machines and devices, 56.9% of our audience agree that identifying DDoS attacks on an IoT network will, as a result, be significantly more challenging.

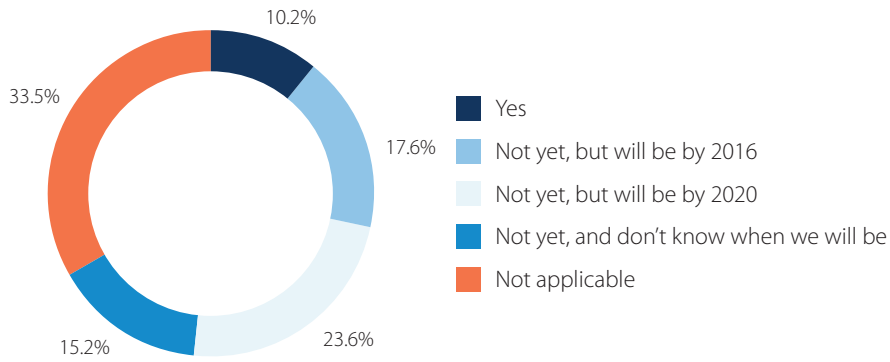
In consideration of the possibility of DDoS attacks on an IoT infrastructure, almost two thirds of our audience (63.6%) reckon that as more enterprise mission critical data gets generated by IoT and stored in the cloud, service providers will be under ever-increasing pressure to ensure availability and network protection. Nearly half (47.1%) of respondents agree that to successfully manage potential risks of traffic spoofing on an IoT network, implementing a cloud-based DDoS mitigation architecture and solution is essential. A similar portion of our audience (47.4%) believes that the introduction of IPv6 will give service providers more opportunity to successfully mitigate the risk of DDoS attacks and spoofed addresses.

47.4%

A similar portion of our audience (47.4%) believes that the introduction of IPv6 will give service providers more opportunity to successfully mitigate the risk of DDoS attacks and spoofed addresses.

15.2%

Nearly a quarter of respondents (23.6%) are targeting 2020 for delivering fully secured IoT services, while 15.2% aren't sure when they'll be able to. A third of respondents (33%) weren't applicable to answer from a service provider perspective.



As a service provider, do you feel that you are ready to deliver a fully secured IoT infrastructure?

65.8% of respondents are sure that a breach or leak of sensitive IoT data is inevitable, and it is interesting to reflect on a data point referenced in the opening section of this survey, which saw 53.5% indicate that security is an afterthought for vendors creating IoT products. As a potential remedy for the immediate security concerns, our audience identified industry associations and collaborative groups as a main source of progress for information security in IoT. Almost three quarters of respondents (70.1%) say industry-wide IoT platform standards are required in order to effectively secure data.

Just 10.2% of respondents believe they are in a position to deliver a fully secured IoT infrastructure today, while 17.6% reckon they will be ready to do so by 2016. Nearly a quarter of respondents (23.6%) are targeting 2020 for delivering fully secured IoT services, while 15.2% aren't sure when they'll be able to. A third of respondents (33%) weren't applicable to answer from a service provider perspective.

It appears as though the operator community wants to jump two-footed into IoT services, unsurprising considering its undoubted revenue potential; however a distinct wariness over data protection is tempering ambition for the time being.

Sponsor Comment

"The momentum being generated by the Internet of Things is only going to continue over the next few years, and there are plenty of reasons why service providers should be excited by the opportunity. Sadly, but not surprisingly, expectations are being tempered due to a perceived lack of protection and information security being provided by the vendor community. The fact that only 10% of the audience considers itself ready to keep the IoT secure indicates how much work is still to be done.

"What remains to be seen is how the entire industry will guarantee the security and protection of information flowing across the network, from the DNS and application layer through to the network core, data centre and cloud. But if we consider the IoT to be more of an era than any one specific technology, then we can identify non-mission critical services and devices for early use-cases, move to ensure their security, then commence an incremental roll-out of live IoT/M2M services. That work is already well under way.

"As much as the surveyed would like standards bodies to solve the security issue, such bodies have a spotty record when it comes to consumer security. Look how long it took for Spam to get under control, or at the ever-growing DDoS problem, or better yet, the hackable home router chaos. If IoT security is to improve, that leadership may have to come from the service providers themselves, who are often at the only strategic point of control in the network."

CLOUD AND IoT

Key takeaways:

- 78% disagree that there is no space for cloud services in IoT
- About 63% think cloud-based apps are more suited to IoT services than on-premise.
- Roughly 70% of respondents think private cloud platforms are more likely to power IoT services because of data privacy / security concerns.
- Respondents are split on the availability of IoT-specific skills in the market.

About IBM:

IBM is a globally integrated technology and consulting company headquartered in Armonk, New York. With operations in more than 170 countries, IBM attracts and retains some of the world's most talented people to help solve problems and provide an edge for businesses, governments and non-profits.

Innovation is at the core of IBM's strategy. The company develops and sells software and systems hardware and a broad range of infrastructure, cloud and consulting services.

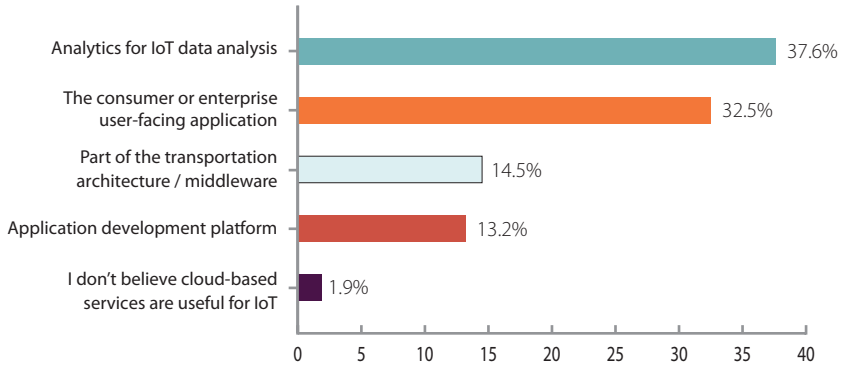
Today, IBM is focused on five growth initiatives – Cloud, Big Data and Analytics, Mobile, Social Business and Security. IBMers are working with customers around the world to apply the company's business consulting, technology and R&D expertise to enable systems of engagement that deliver dynamic insights for businesses and governments worldwide.

For more information, go to www.ibm.com/uk/en/

Cloudy with a chance of IoT

How does cloud figure into the Internet of Things?

Internet of Things (IoT) has firmly moved beyond the hype according to our latest research, but as companies start to consider how to build out the next generation of IoT offerings – products, applications and services – there seems to be no shortage of uncertainty surrounding how developers and IT departments will be impacted, or the likely role for cloud services within IoT. Developers need a robust ecosystem of performant, secure technologies and platforms to develop these offerings, but the consensus around which ones best meet these requirements, and extent of the learning curve involved in developing IoT services – and the requirement to seek out new personnel skilled in a range of different technologies – is still evolving. While developers have already found use for cloud-based services within their IoT offerings, it's equally clear that concerns around security, performance, ease of use and skills may dictate cloud's future role in IoT projects and architectures.



Where do you think cloud-based services will be most useful in IoT?

Are developers sold on cloud for Internet of Things?

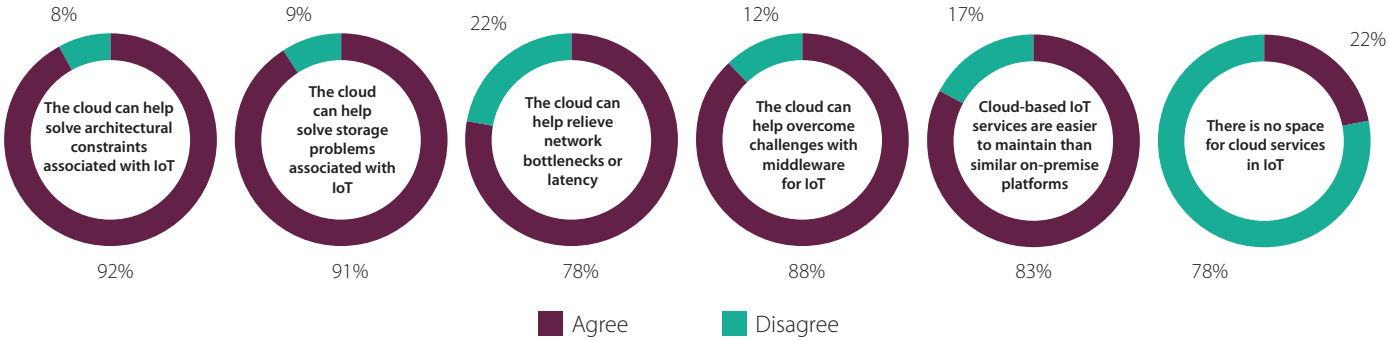
According to our recent BCN and Telecoms.com Cloud and IoT survey, which includes responses from over 651 developers and IT professionals, enterprises are firmly sold on the coupling of IoT and cloud and are well on their way to developing applications and services.

About 65 per cent of respondents agree or strongly agree companies that are slow to integrate cloud – whether at the storage, middleware, ancillary service or application level – into their IoT solutions will fall behind the competition, so it is clear IT organisations themselves see a pivotal role for cloud in IoT. By contrast, 78 per cent disagree or strongly disagree that there is no space for cloud services in IoT.

Where – and in what capacity – cloud will figure into these architectures seems to be a matter of debate, but what is clear is that most believe cloud-based development platforms will be essential for building IoT applications and cloud services. This is, in part, because of efficiency gains and architectural improvements – about 78 per cent of respondents think developing IoT applications and services in the cloud makes it easier to connect up IoT sensors with a series of other cloud-based services.

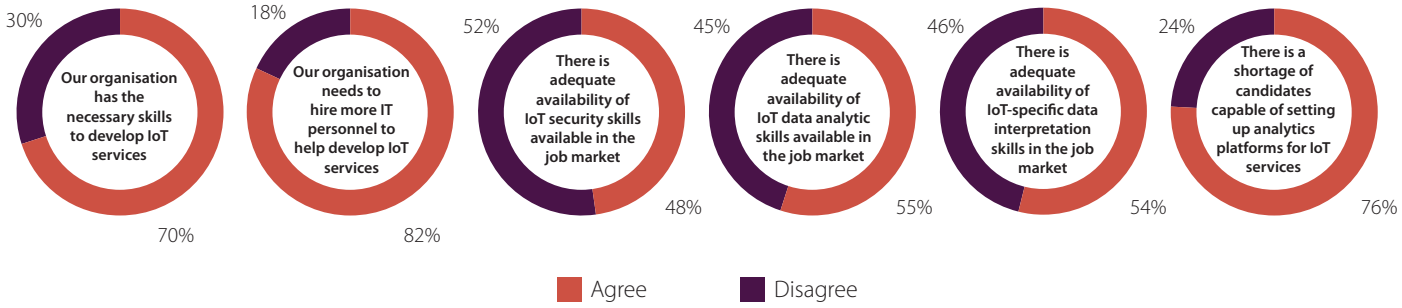
Roughly 35 per cent said their organisations are researching how cloud development platforms can be used in the delivery of IoT products and services, and 19 per cent said they are in the early implementation stages. Just over three quarters of respondents (77 per cent) are either considering, planning to use, or in the early implementation stages of using a cloud-based development platform for their IoT services. It also seems use of cloud-based development platforms for IoT is set to grow in the enterprise. About 36 per cent of respondents believe over half of their organisation will use cloud-based development platforms to create their IoT offerings, and over a quarter (28 per cent) believe that three years from now these platforms will be used by the majority of their organisation.

When looking at cloud at different levels of the stack, three quarters of respondents (74 per cent) believe these services can solve middleware challenges for IoT, 70 per cent believe cloud can help solve architectural constraints associated with delivering IoT applications and services, and 68 per cent agree or strongly agree that cloud can also help solve



Please rate the extent to which you agree with the following statements.

CLOUD AND IoT



Please rate the extent to which you agree with the following statements.

storage problems associated with IoT sensor-generated data and logs. This may be because IoT typically implies the interconnection of a range of devices – potentially speaking an equally broad range of languages – sending data to a centralised repository from the very edge of a network. The importance of robust middleware within that context cannot be stressed enough. Cloud storage is also useful for IoT developers that may not have enough capital to deploy on-premise storage that is scalable enough to meet the demands; with cloud developers can also shard and / or replicate data to a range of different storage services, optimising for any number of variables including latency, proximity to data processing services (i.e. analytics), and cost.

Overall, cloud seems to be the preferred delivery mechanism for a number of applications and services, and IoT is no exception. Roughly 63 per cent think cloud-based applications are more suited to IoT services than on-premise alternatives, which may have much to do with where developers see cloud being most useful in IoT – namely, data analysis. When asked to choose where cloud-based services will be most useful in IoT the top response (38 per cent) was for deploying 'analytics to analyse IoT data', with 'enterprise or consumer-facing application' (33 per cent) coming a close second. Apart from the obvious – that much of the value derived from IoT comes from the insights generated by the data – these results seem to reflect the fact that software connectors to big data services are generally becoming delivered as standardised sets of APIs, and applications of all kinds are increasingly being built as mobile-first web apps. Code maintenance also seems to factor into the equation – about 63 per cent of respondents said cloud-based apps are easier to maintain than their on-premise alternatives.

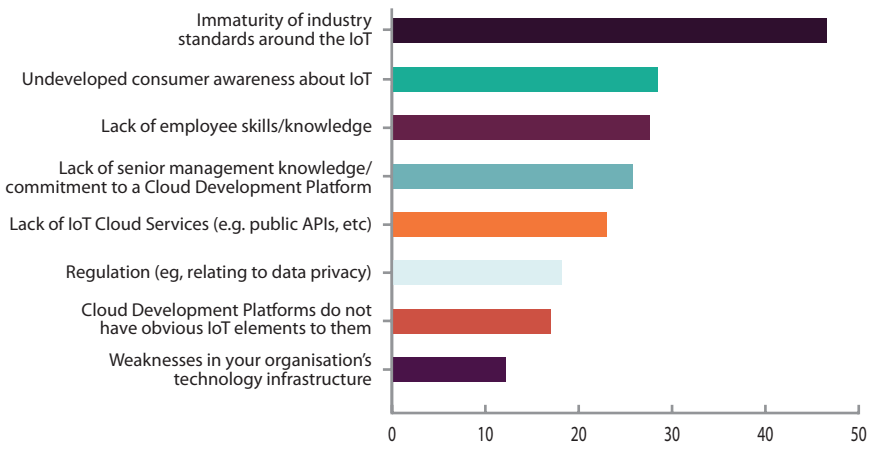
Perhaps unsurprisingly, IoT security seems to be top of mind for IT personnel, especially when it comes to the cloud development platforms being used; indeed, security and data privacy seem to be two dominant recurring themes in cloud more broadly. The top two features respondents are looking for from cloud-based platforms were security (78 per cent said 'very important') and data privacy (73 per cent said 'very important'). But compatibility with a wide range of devices and standards and the ability to support robust data analysis capabilities also rank quite high on the priority list for IT professionals. Nearly two thirds (63 per cent) say protocol and connectivity support for different IoT devices was a 'very important' cloud-based development platform capability, and half of respondents said the same about broad IoT standards support. This speaks to the relative youth of the IoT sector and the fact that there is preciously little consensus on standards.

The growing number and variety of systems and technologies being stitched together to create IoT services today are closed, proprietary systems, and it will take some time for the industry to form best practice and consolidate around open standards.

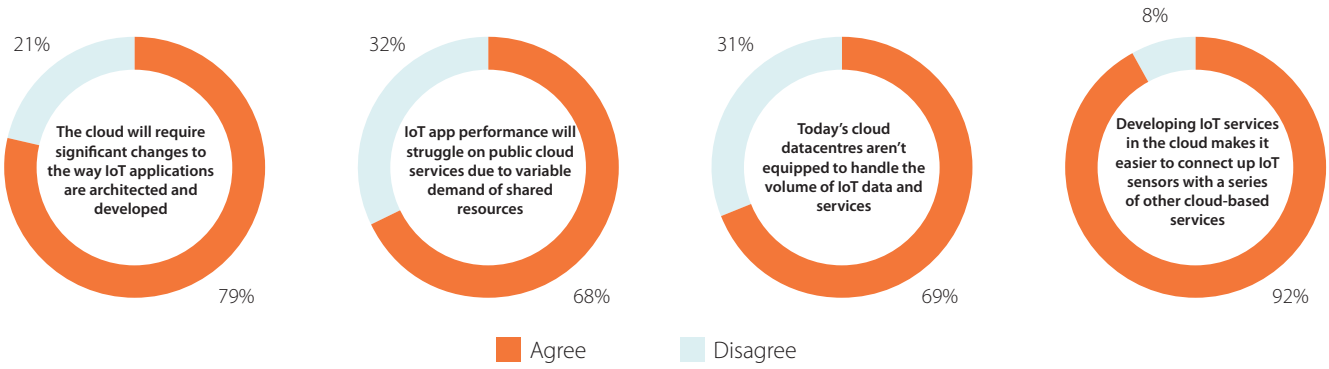
Data analysis support also ranks quite highly among respondents, with close to half saying the ability of cloud-based development platforms to support analysis of large volumes of data is 'very important'. Interestingly, nearly 95 per cent of respondents say it is either 'important' or 'very important' for these platforms to support analysis of data in motion, which suggests developers are overwhelmingly looking to generate insights into their data in real-time from their IoT services.

There's always a 'but' and IoT is no exception

Though it is clear enterprises are sold on the use of cloud for IoT, it is equally clear IT organisations (close to 70 per cent of respondents) see a range of potential inhibitors that may shape the



What are the two chief obstacles to your organisation using a cloud development platform to deliver IoT cloud services?



Please rate the extent to which you agree with the following statements.

architecture and deployment models for these services.

For instance, about 70 per cent of respondents think private cloud platforms are more likely to power IoT services because of data privacy / security concerns; 63 per cent believe IoT app performance will struggle on public cloud services due to variable demand of shared resources; and close to two thirds (about 64 per cent) believe today's cloud datacentres aren't equipped to handle the volume of IoT data and services.

But IT professionals are still concerned about storing and processing IoT data in the cloud. Roughly 63 per cent think cloud for IoT services makes these services inherently less secure or more vulnerable to cyber-attack. And while 55 per cent agree public cloud is secure enough to host data generated from IoT sensors, about a third (32 per cent) of respondents disagree or strongly disagree, so there seems to be little consensus on the role public cloud will play in IoT.

Lastly, standards – or the lack thereof – seem to be a big challenge in this segment. When asked to identity chief obstacles to using a cloud-based IoT platform, the number one response (indicated by 47 per cent of respondents) was 'immaturity of industry standards around the IoT', followed by 'undeveloped consumer awareness about IoT' (28 per cent).

IoT will require new skills, people

Where IT professionals seem to be most split is on the internal availability of skills required of developers and IT organisations to develop IoT services, along with the availability of suitably skilled personnel in the job market.

About 70 per cent of respondents said their organisations need to hire more IT personnel to help develop IoT services; but just over half (56 per cent) said their development teams already have the necessary skills or resources to develop IoT services, and 53 per cent say the skills currently found in their IT departments are transferable to the IoT space.

These results suggest the need for sheer manpower required to deliver additional projects in new areas like IoT outstrips the internal skills gap these enterprises believe they face – but not by much, with 44 per cent claiming their internal IT organisations aren't suitably skilled.

IT professionals are also seem to be split on the availability of personnel skilled in IoT-specific roles in the job market. Respondents were split on whether or not there is adequate availability of operational technology skills to support IoT – slightly more agree (36 per cent) than disagree (35 per cent); on availability of IoT data analytic skills – about 37 per cent don't think there is enough, compared with 32 per cent that believe there is; and on availability of IT development skills to support IoT – about 38 per cent agree there is adequate availability of IT development skills to support IoT in the job market, while 32 per cent disagree.

Respondents were, however, more decided in other areas where capable candidates are lacking: 63 per cent agree or somewhat agree there is a shortage of candidates capable of setting up analytics platforms for IoT services, and close to half don't think there is adequate availability of IoT-specific data interpretation skills in the job market. Given the emphasis on data analytics indicated earlier, the results are slightly worrying, but could also speak to the nascent state of the IoT segment (and the skills and technologies specific to it) not keeping pace with the level of interests being found in organisations. What seems clear given the emphasis on analytics is most consider the insights generated from IoT services to be of extremely high value.

Concluding Thoughts

There is growing interest in the Internet of Things among organisations today and it is clear many IT professionals have set out to create, or are in the process of creating, IoT products, applications and services. There is also a growing consensus that cloud will be a pivotal part of IoT architectures and projects, particularly the development platforms being used to create the services, the applications themselves, and analysis of the data generated by IoT sensors. Many view cloud-based development platforms as a key and growing component of these projects, but it's equally clear developers also see a big role for cloud services in alleviating storage and communications bottlenecks.

But the results of the BCN and Telecoms.com Cloud and IoT survey also suggest IT professionals are deeply worried about standards, something sorely lacking in this nascent space; the ability of datacentre infrastructure to keep pace with the explosion in data processing and storage volume and velocity IoT beckons; and, the security and data privacy implications of cloud in the mix, particularly public cloud when it comes to storing or processing IoT generated data – most seem to be leaning towards private cloud for deployment as a results. Lastly, the results suggest IT organisations are split on the availability of many of the skills required to generate insights from their IoT services and set up IoT projects, and the degree to which IT departments will have to upskill – though more certain that developing IoT services will require more personnel.

NETWORKING CHALLENGES

Key takeaways:

- 62% of respondents believe IoT can't exsit without radio infrastructure managed by operators.
- 33% say cellular coverage and signal strength is the most important IoT enabling feature of the network.
- 70% believe service providers must make full use of real-time data analysis to help IoT reach its full potential.

About Wind River:

Wind River, a wholly owned subsidiary of Intel® Corporation (NASDAQ: INTC), is a global leader in delivering software for the Internet of Things. The company has been pioneering computing inside embedded devices since 1981, and its technology is found in more than 2 billion products. Wind River offers a comprehensive portfolio of solutions for addressing the system-level challenges and opportunities of IoT that is backed by world-class global professional services, award-winning customer support, and a broad partner ecosystem. Wind River delivers the software and expertise that enables the innovation and deployment of safe, secure, and reliable intelligent systems.

To learn more, visit Wind River at www.windriver.com.

Challenges and **opportunities**

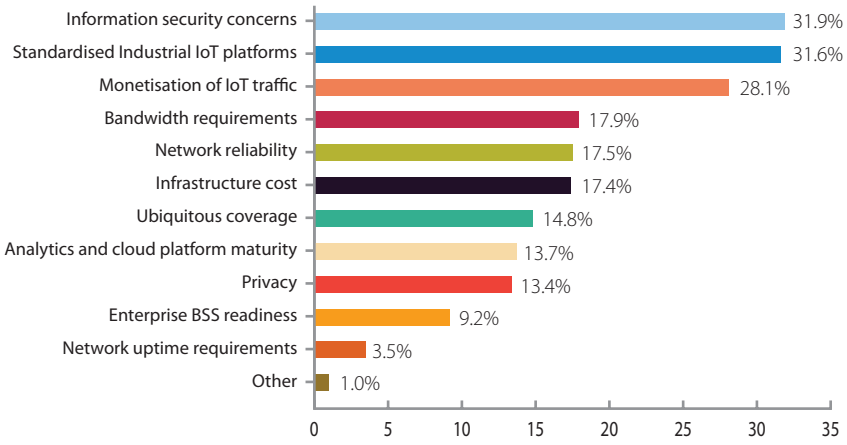
As we wrestle with the definitions, parameters and business models for IoT one aspect is unchallenged: that it will rely on networks, especially wireless ones. The term 'Internet of Things' was devised to evoke a future in which all objects are connected to the internet, so without networks they remain, merely, things.

But today's networks were designed to accommodate computers and landline phones and are already being put under stress by the arrival of tablets, smart TVs and the streaming video demands that accompany them. The addition of billions of new devices, all with unique access needs, connecting to networks is bound to create challenges, and it is these challenges that we explore in this section of the Telecoms.com Intelligence IoT survey.

The first question we asked our respondents was simply what they considered the biggest network challenges for IoT to be. While the ability of the network to cope is a concern, the challenge identified by the largest proportion – 32% – was information security concerns.

The essence of IoT is the exchange of data between connected devices and its intended destination. We still don't know exactly what types of data are likely to be most commonly exchanged, but parts of it will be private, some of it will be extremely sensitive and a lot of it should be of potential use to people other than those it is intended for, be they intelligence agencies, cybercriminals or just mischief-makers. How to secure all this data does indeed seem to be a colossal challenge.

A similar proportion of respondents also identified standardised industrial IoT platforms as a major challenge, with a vision as broad as IoT irreconcilable with a jumble of incompatible proprietary platforms. A close third, chosen by 28% of respondents, was monetisation of IoT traffic, indicating that all other considerations are somewhat academic unless the business case for IoT can be proven. If security was not the number one issue, having a logical business model would certainly rank even higher.



What do you consider to be the two biggest network challenges for IoT?

Our next question asked if the IoT can exist without a radio infrastructure managed by telecoms operators. While the majority of respondents – 62% – said it couldn't, the fact that over a third found the concept of an IoT independent of mobile networks is intriguing. Presumably they imagine wifi, Bluetooth and other short-range wireless connectivity technologies would suffice.

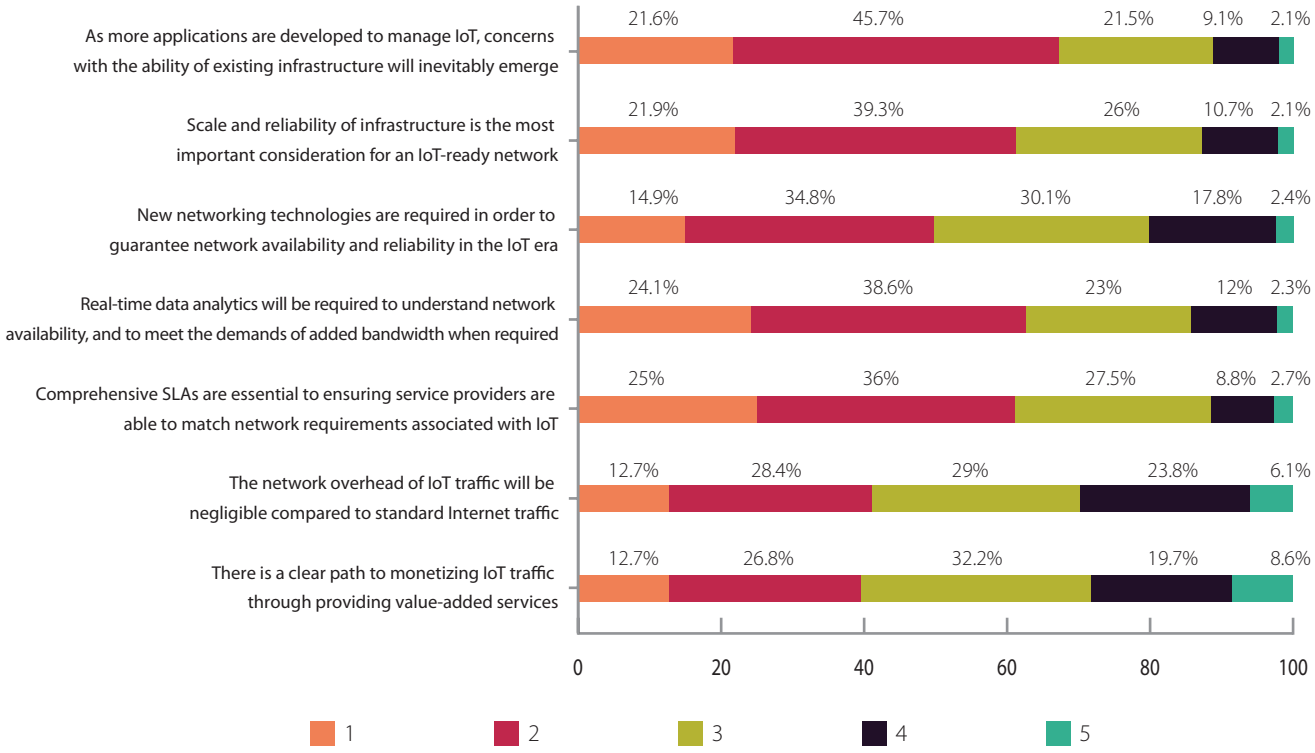
Building on the previous question we then asked what percentage of IoT data traffic respondents thought would be transmitted over mobile networks by 2020. 55% of respondents thought that proportion would be in the 20-60% range, indicating that even in five years' time they expect the majority of IoT data communication to happen over networks other than mobile.

But most respondents accepted that cellular networks will have some role to play, and in our next question we asked them, from a network perspective, what they considered the most important IoT-enabling features. The most popular answer, with a third of respondents, was "Cellular coverage and signal strength", while 17% identified "Bandwidth" as a key feature. The second most popular feature was "Cost efficiency" at 31% and not far behind was "Security", with 26%.

20-60%

55% of respondents thought the proportion of IoT data traffic being transmitted over the mobile network by 2020 would be in the 20-60% range.

NETWORKING CHALLENGES



On a scale of one to five (with 1 being strongly agree and 5 being strongly disagree), please indicate your agreement with the following statements regarding IoT networking challenges.

Having already established that IoT standards are a major concern for our survey, our next question presented a few statements about standards and asked respondents to indicate the degree to which they agreed or disagreed with them. The message here was clear, with 62% of respondents agreeing that "Industry-wide standards cooperation is the only way that IoT can really flourish," while more disagreed with the statement: "Existing standards in place for internet-connected devices will suffice for IoT devices and data," than agreed with it.

A similar format was adopted for our next question, but this time the statements concerned views on network infrastructure from an IoT perspective. The majority of respondents agreed that existing infrastructure will have to adapt to cope with future IoT applications and that it will need to scale reliably to do so. They also agreed that real-time data analytics will be required to enable this and that that network providers need to be held to comprehensive SLAs to ensure they maintain their end of the deal.

With flexibility accepted as a key network feature in the IoT era, our next questions turned to virtualization, one of the key features of which is the greater agility and adaptability it promises networks. We started by asking respondents if they were currently investigating the use of virtualization technology on their network and just over half – 52% – said they were.

We then posed a series of questions regarding virtualization and its possible benefits. There was general agreement that NFV provides the requisite network flexibility and it is an integral feature of an IoT-ready network, but respondents were less convinced by statements indicating a high degree of network automation is required before IoT can flourish.

Our next set of statements concerned network analytics. 70% of respondents agreed that "Service providers will need to access and make use of real-time data analysis to help IoT reach its full potential." However they were less convinced that deep packet inspection technology across the application layer was the best way to acquire that data, but generally disagreed with the statement "The IoT-ready service provider network doesn't need DPI". So service providers are likely to utilize DPI to enable IoT services, but will probably not use the technology for data analytics.

The last question asked in the network challenges section of the survey was the

70%

70% of respondents agreed that "Service providers will need to access and make use of real-time data analysis to help IoT reach its full potential."

perceived readiness. Of those respondents in a position to answer the question, a small majority agreed that, as a service provider, they feel their network is ready to manage the traffic generated by the IoT. As indicated previously, most respondents feel network virtualization and NFV is a prerequisite for IoT. Until NFV achieves greater deployments, service providers will not be ready to properly handle IoT SLAs.

In conclusion it's clear that respondents feel the network faces a number of challenges if it is to cope with the explosion of devices and data consumption that is expected to accompany the growth of IoT.

Standards are a clear concern as it's hard to see IoT achieving what is expected of it via competing proprietary platforms, and even if that challenge is overcome it is unlikely to take off until businesses and consumers have a sufficient degree of confidence in security and the underlying business case.

And while the debate on enabling technologies will continue to run, there is consensus that the kind of flexibility afforded by virtualization will be key and that real-time data analytics will play a major role. The majority of our respondents feel their networks are currently IoT-ready, but those networks will need to evolve on parallel with IoT developments if that's to remain the case.

INDUSTRIAL IoT

Key takeaways:

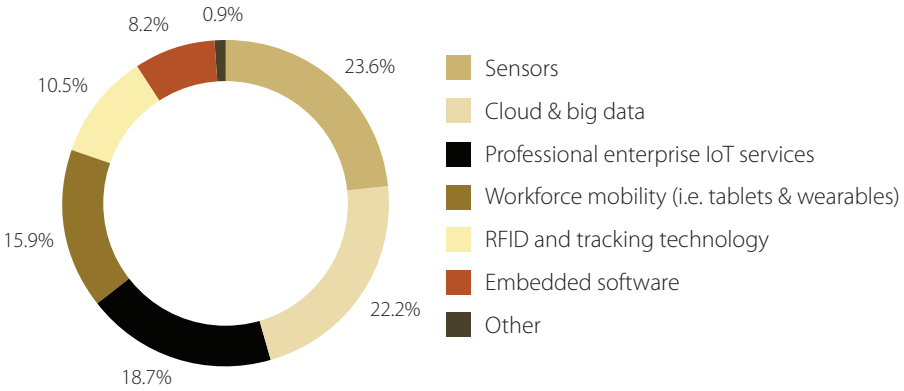
- 50.2% of respondents reckon Industrial will be the most lucrative use-case for IoT.
- 37% believe operational efficiency gains are the primary benefit of IIoT.
- 53.5% reckon IIoT is about making existing assets more efficient.

Industrial techno

Undoubtedly earmarked one of the primary use-cases of IoT in an interconnected world; hopes are high for an internet of things where industrial application takes centre stage. As identified in the opening section of this report, the majority of our audience believes Industrial IoT (IIoT) will become the most lucrative service both for the service provider (47.2%) and for the long term IoT industry in general (50.2%).

To that extent, we wanted to ascertain how IIoT is likely to develop and how the audience views its potential. Our first question in this section of the survey asked respondents to identify, by 2020, what portion of total IoT/M2M revenues will come from industrial IoT. The results indicate that there is still some work to be done before IIoT can be considered to have reached a mature stage where it becomes more lucrative. 79.8% of the audience believes IIoT will comprise up to 50% of all IoT revenues, while just 20.2% of respondents see it being responsible for more than half of all IoT revenues.

The results suggest the audience believes the connected home and more consumer-oriented services are likely to be the principal sources of revenue for IoT until 2020; but when considered alongside our long-term expectations for IIoT, it would seem services beyond 2020 are likely to take off once mature infrastructures are implemented and strategies devised.



Which of the following do you believe will be the biggest revenue generator for Industrial IoT?

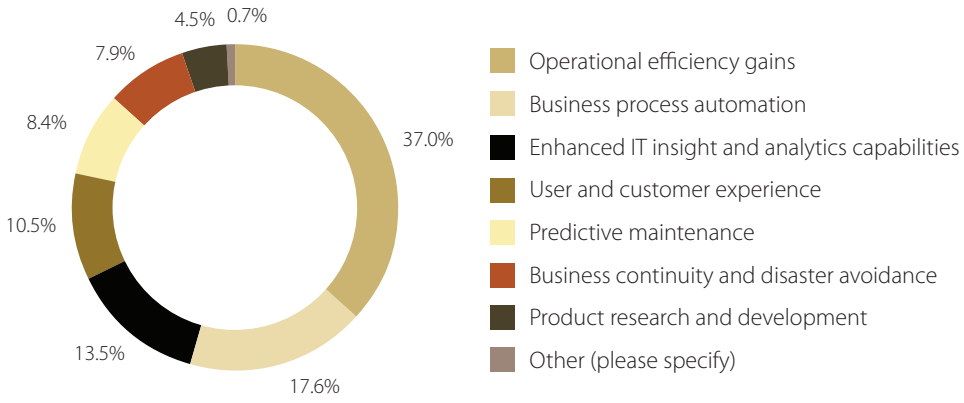
We then asked our audience to identify specifically within IIoT which service will be the biggest revenue generator; and while sensors and cloud & big data received 23.6% and 22.2% of the votes respectively, it was the combination of enterprise facing services which generated nearly one third of responses in total. 18.7% of respondents believe professional enterprise IoT services will be the most lucrative, while 15.9% believe revenues will instead be driven by workforce mobility services through the interconnection of devices and wearables. At the other end, just 8.2% and 10.5% of respondents believe the licensing of embedded software, or RFID and tracking technology respectively, will be valuable and revenue-generating services for IIoT.

When asked about the primary benefit of IIoT to organisations, 37% of respondents identified operational efficiency gains first and foremost, with 17.6% voting for business process automation – which would subsequently lead to efficiency gains. 13.5% believe IIoT will help to better understand IT infrastructure with more intelligent insight and analytics, while 10.5% believe it will greatly benefit customer and user experience.

The implementation of new technology in the enterprise is always met with opposition in the form of challenges which need to be overcome. We asked our audience, service providers only, to identify which barrier to IIoT rollout and success will be the toughest to overcome; and, as previously identified in this survey, standardisation, network challenges and information security came out as the top three challenges (24.1%, 18.3% and 17.6% respectively). Fora exist and are emerging which are dedicated to the standardisation of platforms in an industrial internet of things, and groups such as the Industrial Internet Consortium and the Open Interconnect Consortium are uniting industry, academia and government bodies

79.8%

79.8% of the audience believes IIoT will comprise up to 50% of all IoT revenues, while just 20.2% of respondents see it being responsible for more than half of all IoT revenues.



Which of the following do you think is the primary benefit of Industrial IoT?

in order to successfully bring a level of cohesion, compatibility and interoperability to a variety of platforms emerging in the IoT space.

Meanwhile, it appears the operator community has faith in its own ability to provide the base required for enabling IIoT; as telecoms related challenges such as LTE coverage, BSS readiness and cloud platform maturity ranked at the bottom of the pile of barriers to implementation and monetisation (8%, 7.7% and 6.5% respectively).

When asked which industry vertical is best positioned to benefit from IIoT, and excluding the 18.1% of respondents who identified telecoms; 22.4% believe that utilities firms will best exploit the IIoT opportunity. 17% believe that freight, cargo and logistics firms will be able to best implement IIoT, while 14.0% and 11.8% of respondents think it'll be automotive/ aeronautics and healthcare industries respectively. According to our readers, finance will be the industry which benefits least from IoT, with just 2.6% of votes.

Consumer demand and never-ending data consumption growth continues to put pressure on the telecoms operator, and telcos are increasingly being viewed as a utility instead of a service. As such, the network infrastructure powering today's perennially-connected consumer reaches new echelons of strain and data consumption. Machine-generated data will inevitably add varying amounts of traffic, of significant importance in Industrial IoT, to the service provider network; therefore it is likely that telecoms operators are under more severe pressure to ensure availability and minimise downtime with industrial IoT than consumer IoT, something agreed with by 56.2% of our audience.

53.5%

Speaking of monetisation, 53.5% believe IIoT is focussed on making existing assets more efficient, 40.5% believe it's all about generating revenue channels through new and improved services, while just 6% believe IIoT is primarily focussed on minimising losses.

Just over half of respondents, 50.3%, also believe that operators are the best positioned out of anybody to provide enterprise organisations with IoT-based services, while 47.5% agree that enterprise solutions and professional services will be the primary monetisation opportunities for IoT.

Interestingly, it appears our audience believes the promise of IIoT can be realised with existing LTE-based technology, as 39.9% of respondents disagreed with a forward looking statement saying operators can only monetise IIoT once 5G arrives. Similarly, 44.1% of the audience reckons operators can only make money from IIoT by deploying a comprehensive LTE network for IP traffic.

Speaking of monetisation, 53.5% believe IIoT is focussed on making existing assets more efficient, 40.5% believe it's all about generating revenue channels through new and improved services, while just 6% believe IIoT is primarily focussed on minimising losses.

As with most of the other sections of this report, we finished polling our audience by asking if they feel their business is ready for industrial applications of IoT today. 29.3% said they will be by 2020, 27.5% by next year and 18.3% saying they're ready to do so already. 24.9% aren't sure when they'll be able to introduce IIoT applications.

The distinct optimism surrounding IoT appears to be consistent with some of the views we've received across this report; and the 45.8% of respondents who believe that they'll be ready to run live IIoT applications by 2016, if not before, suggests industrial use-case scenarios for the internet of things will come to fruition more quickly than other consumer-oriented facets of the tech.

About Telecoms.com Intelligence:
Telecoms.com Intelligence, the industry analysis arm of Telecoms.com, works closely with its partners to thoroughly research and create educational services for its readership. In 2014 alone we generated more than 25,000 leads for our clients across more than 50 campaigns.

A consultative and collaborative approach with our dedicated analysis team ensures the creation of truly unique content, highly regarded throughout the industry. Telecoms.com Intelligence services combine statistical analysis and broad industry knowledge to effectively deliver insight and analysis through the use of webinars, bespoke surveys, white papers and more. All campaigns are supported with extensive marketing campaigns, to guarantee quantifiable business leads for our clients.

Since its launch in 2001, Telecoms.com attracts more than 86,000 unique visitors and 173,000 page views on a monthly basis. The recently redesigned website also provides a newer and easier-to-navigate resource directory from which to access Intelligence content.

For more information, visit http://www.telecoms.com