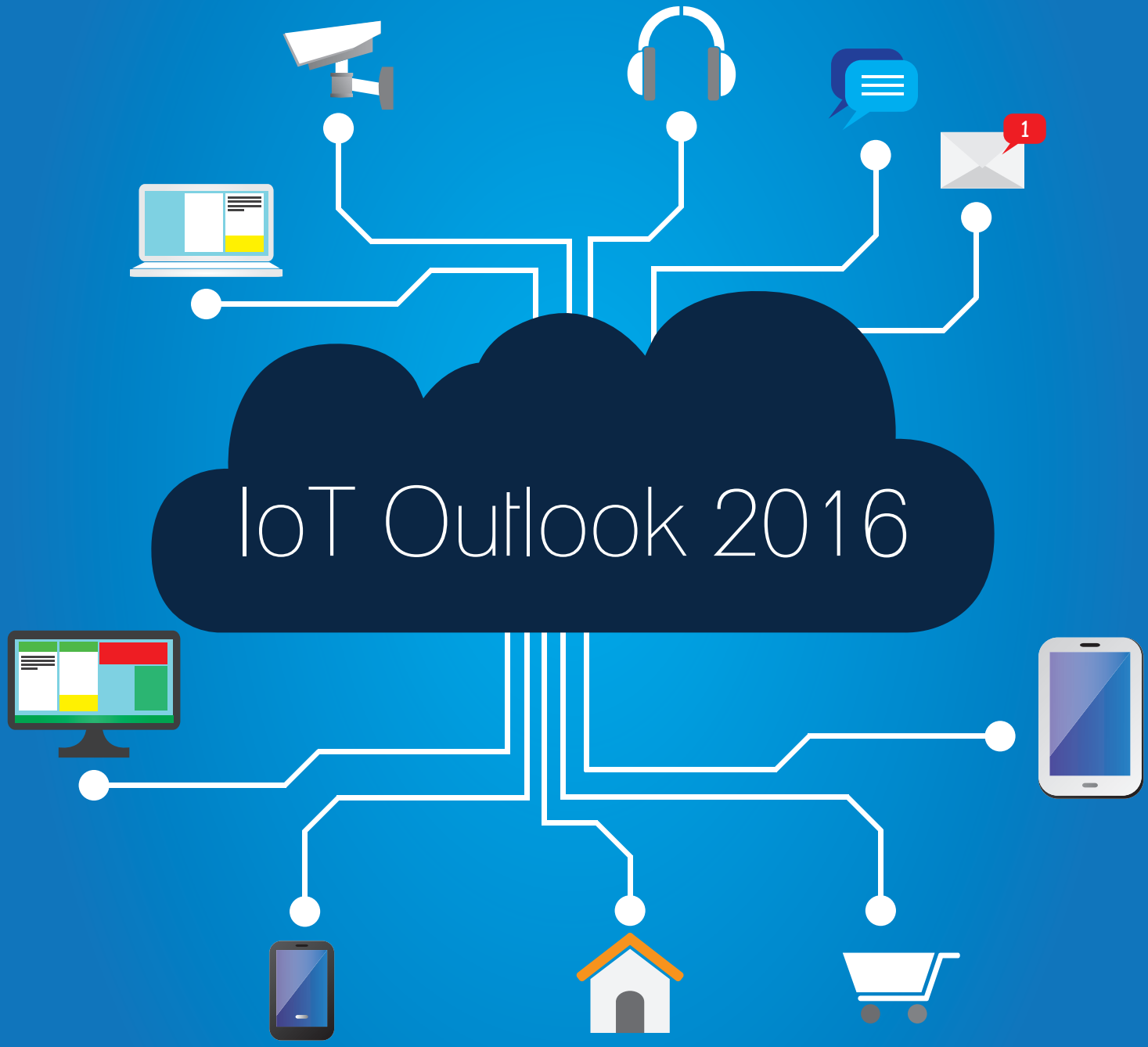
telecoms.com INTELLIGENCE



IoT Outlook 2016

Sponsored by

gemalto security to be free

aeris

f5

STARHOME MACH

Contents

Welcome

Time for things to change

It is easy to lose perspective on how rapidly the technology industry has developed in recent times, but the strides being made in the ecosystem around the Internet of Things have been significant over the past 12 months.

Partnerships are beginning to be forged between operators, vendors and protocol-developing organisations such as LoRa and Sigfox, as national and international roll outs loom large.

Because this industry is moving at a ferocious pace, perhaps more than any other this industry is currently witnessing, Telecoms.com deemed it necessary to conduct a thorough review of where the market is today and what the road ahead will likely look like. Last year's IoT Outlook report highlighted monetisation considerations as one of the biggest challenges, and so this year we looked to assess the progress made by the audience as we look to move from developing use cases to live network deployments.

The report yielded some surprising results, many of which indicate the foundations of a promising road ahead being built, with many technological and business factors being addressed and resolved today.

With 900 respondents to the survey, this year's report focuses on six specific areas of IoT; starting off with a review of the overall market, before deep-diving into specific areas including IoT platforms, security, connectivity, industrial and consumer IoT offerings like the smart home and connected cars.

With the speed of technological innovation refusing to relent, perhaps in five or ten years from now we will be taking IoT for granted as part of our daily lives.

We hope you find this report a useful guide in your IoT journey.

Many thanks,

Tim Skinner
Head of Telecoms.com Intelligence
Telecoms.com

gemalto
security to be free

NAVIGATING THE IOT LANDSCAPE

Key takeaways:

- Roughly four in five respondents believe there is a lack of consensus over the best way to strategise, deploy and monetise IoT.
- More than half the audience says IoT and M2M have now come to mean the same thing.
- IoT services will be responsible for up to 50% of business revenue by 2020, according to half the audience.

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.

Things can only get better

Welcome to the Telecoms.com Intelligence 2016 IoT Outlook, our extensive and in-depth analysis of the rapidly developing landscape evolving around the internet of things. Following our first version of the report last year, we polled close to 1,000 industry professionals on a variety of subjects which will define how the IoT will flourish, if indeed it does go on to deliver on its early promise. The results will be thoroughly laid out and analysed in this report, covering the overall landscape, cloud computing, data analysis, connectivity and security as well as snapshots of the market opportunities which exist within the industrial and commercial sub-sections of IoT.

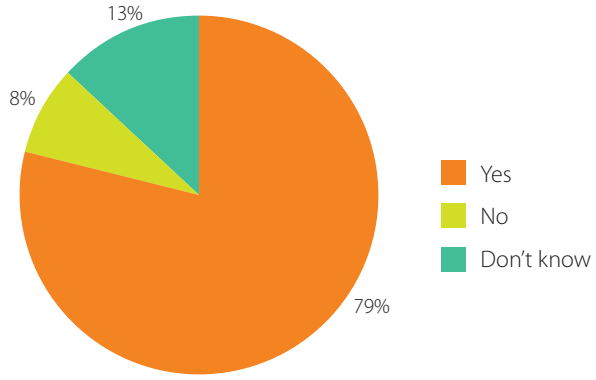
From a marketing perspective, the internet of things is lining up to be one of the most dominant tech trends for the next ten years; with technology players from a veritable buffet of industries convinced it will redefine how businesses operate and deliver services. From a more granular perspective, a shroud of mystery still exists over IoT, with a variety of network and connectivity challenges associated with making it the all-encompassing technology it promises to be.

Before we make the dive into aforementioned areas of analysis – cloud, connectivity, security, industrial and consumer – we will first deliver an overview of the marketplace today and understand broader attitudes relating to the IoT industry.

Let's begin by clarifying the profile of our respondents.

Of the roughly 1,000 respondents we received for our survey, exactly 50% came from the service provider community – including MNOs, cable operators, ISPs, multiplay operators, broadcasters and cloud service providers. Service providers are frequently referred to as the great enablers of IoT, and thus represents the primary market for this study.

The second greatest group of respondents after service providers represent suppliers of IoT services, with 17% - this group includes hardware, software, services and application development vendors. Consultancy, analyst or research firms made up an additional 14%, while the remaining fifth of respondents originated from a range of sources including more niched telecoms services, government agencies, education institutions and industrial end-users of IoT technology.



Do you believe there's a lack of common consensus over the best way to deploy and monetise IoT?

The broad array of respondents to this survey serves to represent the far-reaching impact the internet of things will have, and therefore helps to further illustrate the enormous opportunity which exists for the operator community delivering the technology.

In terms of the day-to-day job functions of our audience, just short of half of all respondents are involved with the technical running of infrastructure, IT, network operations or R&D elements within their organization. Roughly a quarter come from sales and marketing roles, 13% from corporate management and another 11% coming from consultants or analysts. There is also 10% of the audience which comes from miscellaneous functions, including finance and corporate governance, and so on.

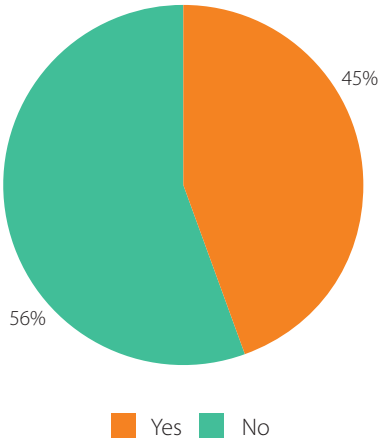
Finally, the geographic profile of respondents sees a statistically significant global representation despite a European primary market worth roughly 40%. The remaining three fifths of respondents are almost perfectly split across APAC, MENA and both North and Latin America.

With operator respondents originating from varying geographies and backgrounds, we sought to understand whether dedicated M2M or IoT departments have been established within their respective companies. The question yielded a 40/60 yes/no split, suggesting that despite an awareness of IoT, organizations are yet to go all in on a dedicated strategy for it.

Further clarity as to why this might be the case was suitably illustrated by the results of the subsequent questions asked in the IoT Landscape. A considerable majority, 79% of our audience, believes a lack of common consensus over the best way to deploy and monetise IoT still exists. Considering this is such a sizeable percentage of the audience, a precedent is already being established in that we're still at a relatively infantile stage of development for IoT, and a level of confusion exists about how to proceed in developing a serious proposition.

This general lack of consensus can be further explored when we look at the responses to a question which asked users to identify what they most commonly associate with the term IoT. A range of responses highlighted a further lack of consistency in what IoT means to the audience. 26% mainly associate IoT with smart cities; 21% smart home and another 18% looking more at enterprise applications by citing business efficiency.

With the three most commonly identified answers representing three differing elements of IoT (societal, consumer and



Do you believe the terms 'IoT' and 'M2M' have come to mean the same thing?

industrial), our earlier assertion is reinforced. Other notable responses include embedded industrial applications (13%), connected cars (9%) and smart metering (8%).

It is evident that a general lack of consensus exists over what IoT really is, and in its early stages has often been conflated with M2M (machine-to-machine). 45% of respondents believe that IoT and M2M have now come to mean the same thing. Alas, a conclusive definition of the difference between the two is hard to come by. Some deem M2M to be the predecessor to IoT, considering the former to be the rudimentary connection between devices with little in the way of dedicated infrastructural, security or data analysis tools or other enabling features which will help make IoT the broad and comprehensive set of communications systems it promises to become. Others say IoT is just a souped-up term for M2M, the appeal of which appears to be diminishing for marketers with the emergence of a newer and sexier buzzword.

Whichever definition the individual attaches to IoT, our collective of individuals is already actively generating revenue from it in one way or another, and expects to increasingly do so as we approach the milestone of 2020.

In the next 12 months, just under half of our respondents expect to generate between zero and 10% of their revenues from IoT. Elsewhere, less than one fifth expects IoT to generate 10-30% of revenues, less than one tenth says up to 50%, and less than 5% expect to be able to attribute IoT with more than half of their total revenues in the next year.

Fast forward to 2020, however, and that revenue-generation expectation changes significantly. More than half of all respondents expect IoT to be responsible for somewhere between 10% and 50% of their total business, while 17% believe it will be 10% or less. A further 16% say more than half of their business will be directly concerned with IoT, and 15% opted against mustering a best-guess effort.

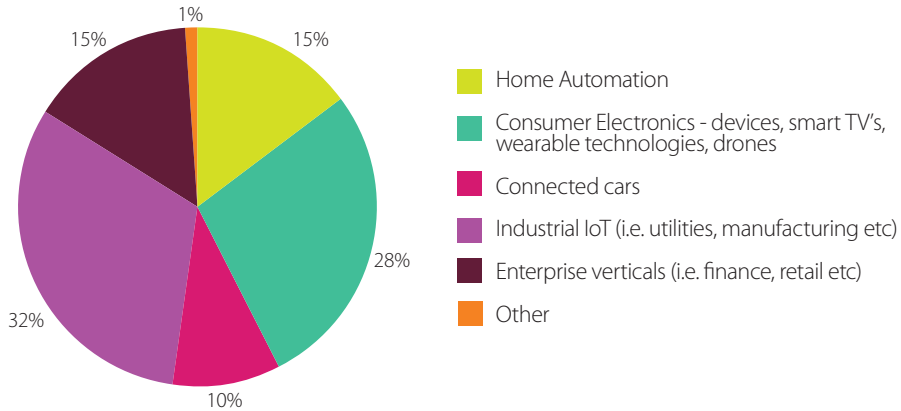
With this survey being a largely operator-centric exercise, one is not too surprised to see one in five respondents say telecoms operators are best positioned to provide IoT services. It is perhaps more indicative to see a hefty chunk of respondents opt for a more collaborative answer to the same question, with half our audience saying the best IoT proposition will come from a mix of operators, infrastructure and IT vendors, systems integrators and specialist IoT service providers. We can hark back to our earlier conclusion that more collaboration and broader definition of IoT is required, and that is an effort which the entire industry can get behind to ensure the comprehensive definition of IoT and sufficiently educate the market over its potential.

Beyond trying to figure out which company in the IoT realm is best positioned to monetise it, we sought to understand which specific service the audience believes comes with the biggest value proposition attached. Between them, Industrial IoT (such as utilities and manufacturing) alongside enterprise vertical applications (such as finance or retail) garnered just under half the votes from respondents – 32% and 15% respectively. It is the consumer-facing element of IoT which the audience marginally has greater hopes for, however, with consumer electronics, home automation and connected cars generating 28%, 15% and 10% respectively to a total of 53%.

With wearable technology threatening to pose a genuine value proposition to the consumer, and it looks like it could for the mass market given enough time, we then looked to get a bit more granular and asked specifically which market segment will be most impacted by wearable technology. We did not specify exactly what form of wearable we are considering in this regard, just general wearables like smart watches, Fitbits, smart glasses etc.

The market segment our readers feel will be most affected by wearable technology, by some distance, is the health and fitness market – which gained 45% of the votes. Access control gained 28%, encompassing enterprise identification, building access or for domestic residences. Contactless payments has been a rapidly developing industry in recent years and with the advent of various mobile payment services such as Apple Pay, Samsung Pay and Android Pay - which have either already hit the European market or are due to in 2016 - comes greater opportunity for the integration of m-payments with wearable technology. 17% of the audience reckons payments will be the market most impacted by wearables. Finally, transport was identified by around 10% of the audience.

Leaving to one side the more beneficial aspects of IoT, of which there are many as discussed, what are the biggest inhibitors to the monetization of the technology? The audience firmly believes that security is the challenge which requires the most addressing, and by some distance. More



Which IoT industry segment do you see as most lucrative for service providers?

than a third (34%) cite issues revolving around securing the entire IoT stack is the biggest inhibitor, while just under a quarter (24%) said conflicts emerging in the standardization realm pose the largest threat. An identical trend was observed in last year's survey to the same question, with security and standardization occupying the top two challenges; which indicates we're yet to make resounding progress in resolving either over the past 12 months.

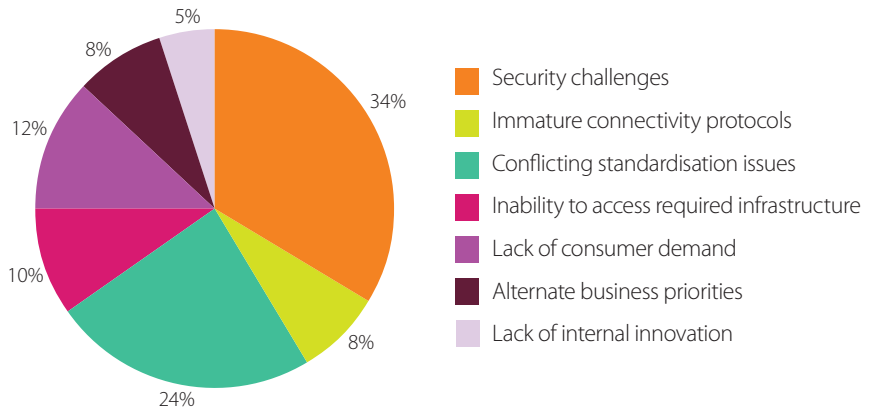
Other responses of note include a lack of consumer demand (12%), a lack of access to the required infrastructure to deploy IoT (10%), an immaturity in connectivity protocols (8%) and alternate business priorities (8%).

Coming back to security, though, and the penultimate question of this section sought to ascertain which market segment is the most sensitive to security issues. For this question we allowed the audience to choose all segments they deemed appropriate – and with a total of more than 1,800 responses on this question we saw IoT-based payment technology as the overwhelming security concern.

The remaining answers were relatively closely grouped, but none gaining quite the same level of attention as the 80% given to payments by the audience; but smart home technology, automotive, health and fitness, smart grid and transport technologies all gained between 24% and 36% of responses. The results yielded by this question reaffirm a common opinion that financial risk can result in the most disastrous consequences for organizations and the most risk-averse providers of IoT will naturally delay the rollout of payments solutions until security concerns from device to bank are appropriately allayed.

The final question in this section asked respondents to state their level of agreement with a variety of statements on how the internet of things will take shape. The statement which gained a 93% agreement rating (categorised as either "agree" or "strongly agree") took a more customer-centric approach, and said "the main purpose of IoT is to improve consumer quality of life". The second most commonly agreed with statement drew an 86% rating, saying that IoT is designed to make businesses more efficient. While statements surrounding the IoT-enabling properties of 5G and IoT's ability to lower the barriers between vertical industries generated similarly high levels of agreement from our readers, our final statement which said IoT will be the single most significant technology trend of the next decade drew the highest disagreement rating of any other. 31% either disagreed or highly disagreed.

That, therefore, draws a close to the opening section of this year's IoT Outlook report, and paints a picture of an industry keen to jump two footed into IoT and all of its M2M-ish glory while simultaneously having its ambitions tempered by significant security concerns and confusion on how to develop a winning strategy. The rest of this report will touch upon each of the main areas identified in this opening section, including security, connectivity, cloud computing and data analytics – while we'll also shed some light on the potential of both consumer and industrial IoT. We hope you find it useful.



What do you consider to be the biggest inhibitor to monetising IoT?

Sponsor's Comment

Internet of Things is turning from hype to reality. M2M took centre-stage for a good part of the last decade, and has now become a mature market. So, there's little surprise that 45% of respondents see little difference between M2M and IoT. With consumer electronics heavyweights stepping up to connect more than just smartphones, the vision of a more connected society is transcending enterprise and industrial usage to the consumer world as well.

Regardless of the segment, industrial or consumer, successful IoT applications require collaboration of multiple industry players. Nearly 50% respondents agreed that IoT services are best provided by a collaborated effort, which reinforces the industry's understanding of this precursor to success. In order for such collaborations to work, three capabilities are imperative: connectivity, security and monetization.

Connectivity has already matured significantly, and with 5G round the corner, bandwidth and latency will be optimised even further. Connectivity infrastructure, now, needs to focus on quality of service and experience, with smart objects in mind. This is paramount for developing IoT applications that truly deliver enhanced user experience, and gain consumers' trust to increase IoT adoption.

This leads to security, which is pivotal for the ecosystem to thrive, and for users and enablers to have trust in each other. Security breaches, whether on devices, on the cloud or on the network, can be a big hurdle to the adoption of IoT. Finally, another important capability is monetization – across the value chain. Nearly 80% respondents feel there's a lack of common consensus to monetise IoT. The monetization structure should allow all stakeholders in the value chain, whether OEM, MNO, ISV or CSP, to monetise their IoT assets through new business models.

Gemalto harnesses its experience of working with enterprises, cloud service providers, governments, financial institutions, OEM and mobile network operators to enable trustworthy connected digital ecosystems. To learn how Gemalto can help your business connect, secure and monetise your IoT assets, visit our website www.gemalto.com/iot, or write to us at iot.query@gemalto.com.

CLOUD PLATFORMS FOR IOT

Key takeaways:

- 49% of respondents say data analytics is the most important feature of an IoT platform.
- IoT services will mostly be built in-house instead of outsourced to third-party vendors, according to 70% of the audience.
- Two thirds of respondents believe 5G will be the main connectivity platform for IoT, when it arrives.

About Aeris:

Aeris is a pioneer and leader in the market of the Internet of Things – as an operator of end-to-end IoT and machine-to-machine (M2M) services and as a technology provider enabling other operators to build profitable IoT businesses. Among our customers are the most demanding users of IoT services today, including Hyundai, Acura, Rand McNally, Leica, and Sprint. Through our technology platform and dedicated IoT and M2M services, we strive to fundamentally improve their businesses – by dramatically reducing costs, improving operational efficiency, reducing time-to-market, and enabling new revenue streams.

For more information, go to www.aeris.com.

A platform for greatness

The connectivity of IoT devices and sensors presents opportunity in abundance but, with it, substantial challenges in how network operators and enterprise companies alike assure and manage device connectivity while gleaning valuable insight from the data being transmitted. After all, what is the purpose of making these M2M connections without fully understanding what is happening, and being able to analyse areas where we can boost value further? Furthermore, is the traditional network even capable of managing the pure volume of traffic the internet of things is expected to produce?

With a variety of cellular connectivity platforms emerging and cloud computing continuing to promise the sort of agility and flexibility, IoT will likely need, this section of the survey sought to understand attitudes towards the characteristics required from an IoT-facilitating platform.

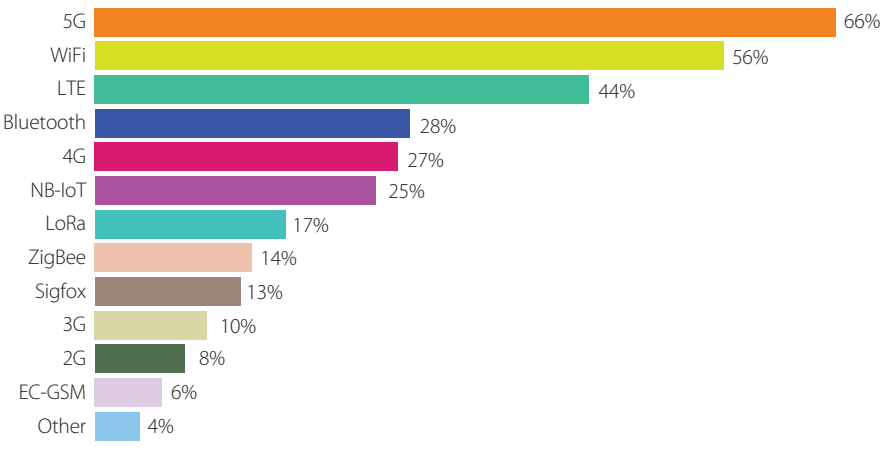
The first question in this section looked to establish potential front runners from the plethora of connectivity options promising to shape the future of IoT. The audience was asked to identify which protocol would have the biggest impact and thus prevail as the predominant enabling-technology. Respondents were asked to select as many options as they saw fit, and as we can see from the accompanying graphic, 5G was deemed to be the most promising – despite the very long road ahead before any form of 5G becomes tangible let alone a commercial reality.

Nevertheless, there is strong support from our audience for 5G as the principal connectivity form for IoT – 66% no less. However, a similarly large proportion of the audience also selected a more immediately viable technology in the form of Wi-Fi, chosen by 56% of the audience.

Wi-Fi operates in the 2.4GHz or 5GHz bands, a high frequency for devices with low payloads. With that in mind, the Wi-Fi Alliance recently announced plans to adopt a lower frequency and separate standard in the name of enabling IoT connectivity. According to the Wi-Fi Alliance, a shift to 900MHz using unlicensed spectrum will suit smaller, IoT-ready devices consuming less power and bandwidth to communicate. In short, the change in standards will be better tailored to lower-end IoT devices found in the readily accessible consumer market.

Elsewhere, LTE appears to be a favoured connectivity technology among our audience, with 44%. Perhaps unsurprisingly, the audience didn't seem to hold out much hope for Sigfox, the parallel low-power WAN protocol on the rise to IoT prominence presenting a threat to operator-owned cellular networks. The technology is gaining traction among companies looking to connect very low power and dumb devices which require the most rudimentary connectivity, with various global operators partnering with it so far. In today's technology industries there's a growing precedent for consolidation and with a number of conflicting standards in the LP-WAN space – including Sigfox, LoRA, Weightless and NB-IoT – there could be a fight for the top spot.

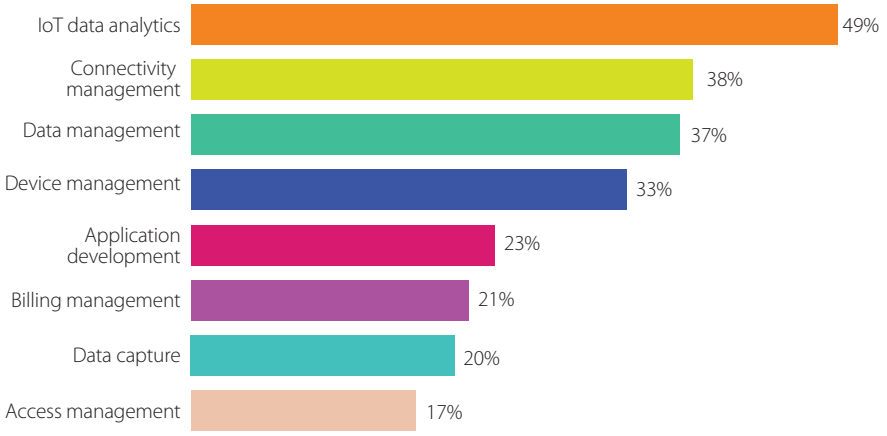
Moving on to our second question, we asked the audience to identify the most important characteristic of an IoT PaaS (Platform as a Service) for their organisation. Again, as we saw in the IoT Landscape section of the report, security



Which of the following do you think will become the main connectivity technology enabling IoT?

"In today's technology industries there's a growing precedent for consolidation and with a number of conflicting standards in the LP-WAN space there could be a fight for top spot."

CLOUD PLATFORMS FOR IOT



Which platform capability is most important to your IoT service

Many argue that IoT is an extension of M2M with more advanced analytics power and intelligence attached to the service.

and data privacy topped the list for respondents – with 43%. A core bunch of the most popular answers after security related closely to assuring and enhancing service delivery; with faster time-to-market (29%), reduced service delivery costs (23%), scalability for service growth (23%) and reliability and performance (23%) following up.

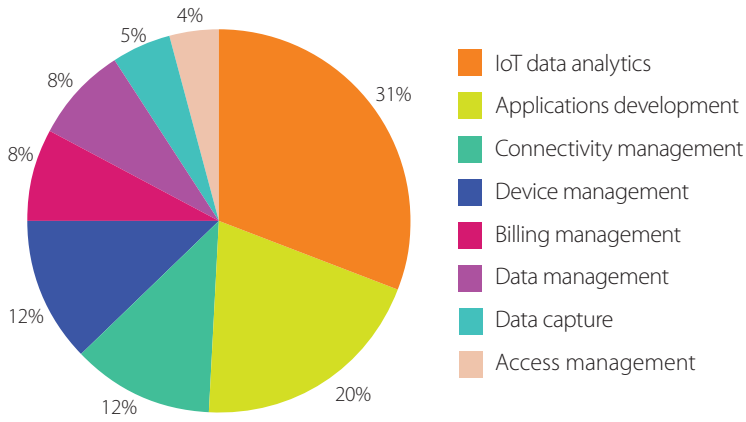
Beyond characteristics of cloud IoT PaaS, we also asked which specific function or service is most important. By some distance, the most important feature identified by our audience was IoT data analytics, as stated by 49% of respondents when asked to pick three features. Following up close to one another saw connectivity, data and device management capabilities selected by respondents as important features of an IoT-ready PaaS – 38%, 37% and 33% respectively.

The overwhelming response in favour of big data leads on to the next question of this section which looked to understand various attitudes towards analytics for IoT. Many argue that IoT is an extension of M2M with more advanced analytics power and intelligence attached to the service, and the majority of our audience believe IoT is simply not possible without using sophisticated data capture and analysis services – a view agreed with by 58% of respondents. A further third of respondents said they need to use some data analytics software to gain some understanding of how IoT is being used by customers or to optimise a deployment. Meanwhile, less than one in ten (9%) of the audience believe analytics is a luxury, with basic connectivity always being the priority.

But with the need for big data and suitable analytics capabilities comes a big need for cloud infrastructure capable of managing it. When asked how important cloud-based platforms will become to the future success of IoT, 62% of the audience deemed it either vital or very important; inferring that cloud platforms will be used in the majority or all parts of the delivery of IoT services. On the whole, a vast majority of the audience said you can't do IoT without cloud computing facilitating it in the background, with an additional 26% of respondents saying roughly half of all IoT platforms or services they plan to offer will be based on cloud technology. Just 12% said there will be a little-to-no need for cloud in IoT.

With optimism abound for IoT platforms, and the need for cloud systems in place to support them sufficiently identified, we wanted to understand hesitancies or barriers preventing users from building IoT applications internally. The results yielded a conclusion hinting towards a lack of people-related skills and the need for additional training in order to productively construct bespoke applications. 42% cited a lack of expertise to integrate with other applications and systems; 39% said there's a lack of knowledge or skills required to build applications; 24% said there's a general deficit of knowledge on how to create and manage rules, events or triggers which require further action; while another 22% said they don't know how to manage and visualise data. All of which suggests a broadly unqualified technical workforce not being entirely sure on how to proceed with IoT in their organisations, symptomatic of the relatively infantile stage of IoT at which we find ourselves.

With that in mind, the audience was then quizzed on which capabilities they would most likely outsource to a third party instead of taking on in-house. Most commonly identified was IoT data analytics, selected by 31% of respondents,



Which platform capability are you most likely to utilise from a 3rd party instead of building in-house?

which would suggest a fair percentage of IoT adopters see this core function as one which, given its previously ascertained importance, they would prefer to have bound to SLAs to guarantee the quality of service. Analytics was followed by application development with one fifth of all responses, with the management of connectivity, devices, billing and data receiving 12%, 12%, 8% and 8% respectively.

With a level of willingness to deploy services through the use of a third party, we sought to understand how much in-house implementation of IoT solutions users will likely be taking on themselves compared to outsourcing externally. The answers indicate a high level of willingness to relinquish control of building an IoT solution to various suppliers.

A fairly sizeable lack of expertise is preventing users from really harnessing the IoT opportunity in terms of creating bespoke and unique applications.

19% of the audience want to outsource the entire IoT solution-building process with help from a solutions provider or systems integrator. The majority of respondents, 42% said they want to build solutions inside their organisation using many best of breed white-label solutions from third parties, with an additional 28% saying they would do the same but with a relatively limited number of external solutions. A brave 12% of the audience say they want to keep full control of the process and build every element of an IoT solution internally.

In conclusion, what this section of the survey indicates to us is a fairly sizeable lack of expertise is preventing users from really harnessing the IoT opportunity in terms of creating bespoke and unique applications. There's a willingness to relinquish control of the application development process to third party vendors, but with it comes an implicit trust that the output yielded will be secure, stable and of a high enough quality to push to end-users.

There's a level of confidence that the increasingly mature cloud computing industry will provide the agility and flexibility required to run the data analytics services necessary to fully harness the potential of IoT, but again a reluctance to do so in-house as a result of a lack of expertise. The industry, therefore, will likely require a sizeable time and financial investment to educate IT and engineering staff with the knowledge and skills to make the most of the significant opportunity in front of them.

Sponsor's Comment

As the value of the Internet of Things (IoT) becomes apparent, more and more companies are increasing their efforts to take seemingly disparate, lower-value, unconnected products and transform them into a connected service that offers broader value. However, the journey to this transformation is full of complexity characterised by unclear objectives, a lack of expertise/skills, and multiple technologies.

We believe that regardless of the vendor or technology an enterprise might select, each business has to ensure that it incorporates a few important services as it seeks to transform unconnected products into a complete IoT service(s).

The most fundamental element of a connected product is sensors in a device(s) or machines that talk to each other and also to a central application, so choosing a connectivity management platform to transport data for further action and analysis is a critical first step.

Next, the data sent from the connected devices needs to communicate with applications built to interpret the data and implement actions. This can be accomplished with an application enablement platform used to store the vast amount of data generated and manage it so other services can make access of it.

Thirdly, a remote device management platform is needed to support secure administrative activities such as accurate inventory of devices, remote configuration and diagnostics.

Lastly, IoT applications serve the most critical of functions and help unlock the IoT opportunity as every connected device must have an associated application.

Here are a few additional considerations:

- Buy vs. build: Buying end-to-end service vs best-in-breed approach
- Security: Balance the right mix of security, performance, cost and time-to-market
- Scalability: Service architecture and solution that is aligned with the Internet
- Cost: Minimise costs at the IoT deployment scales

We hope this report provides guidance in your journey to garner value from the Internet of Things. Happy reading!

OPTIMISING IOT CONNECTIVITY

Key takeaways:

- More than half the audience plans on using their existing radio network for both people and machine-based communications.
- Nearly 90% of respondents see permanent roaming as a major challenge for businesses providing IoT services.
- The radio network will carry up to 50% of IoT traffic in the future, according to nearly two thirds of the audience.

About Starhome Mach:

Starhome Mach is a market leader in value added global mobility and clearing services, removing communication barriers and differentiating services for people and connected devices.

We have harnessed our vase expertise in global connectivity technologies to develop next-generation M2M/IoT solutions that provide robust operations and business layers far beyond what is currently possible in the market.

These capabilities optimize costs and QoS, manage and maximize APRU and support scale-up of the MNO's IoT business, while ensuring services can be tailored to enterprise needs.

Starhome Mach's customer base comprises over 300 mobile network operators including 24 leading groups.

Connecting things

So far in this report we have analysed the overall IoT landscape, the future proposition for operators as well as the level of necessity of cloud-based platforms to enable the development and deployment of IoT services.

This section of the survey will focus on the various elements involved with providing and optimising connectivity to IoT devices, from radio access requirements to enterprise devices. A perennial challenge for telecoms operators, including and excluding IoT, is gaining visibility on the activity and identity of specific devices operating or gaining access to the network.

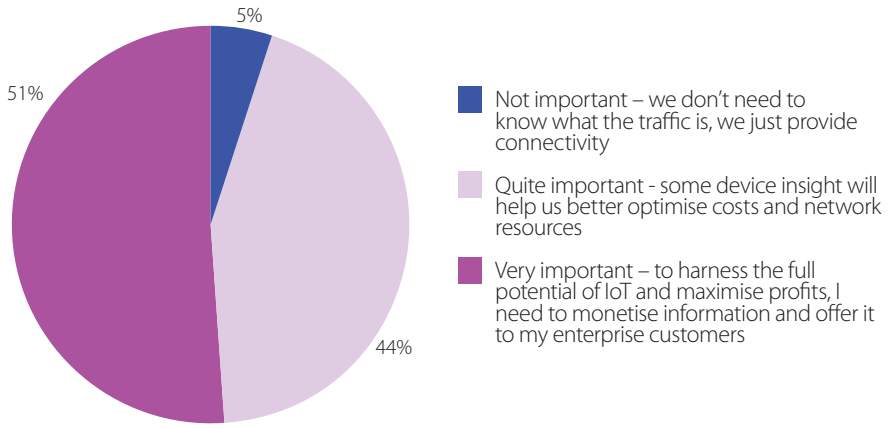
In the context of IoT, gaining such insight could allow operators to manage their networks in optimal fashion, such as allocating appropriate bandwidth or prioritising certain traffic types in certain contexts. With that in mind, the first question we posed to our respondents for this section looked to ascertain the perceived importance of establishing strong insights into device activity, identity or requirements on a granular level.

In this case, more than half of the audience stated that having this ability is very important, stating "to harness the full potential of IoT and maximise profits, I need to monetise this information and offer it to my enterprise customers". This very revenue-centric approach to IoT device management received 51% of votes from the audience, while a more network quality-related point of view also gained a substantial portion of responses. 44% said having the ability to gain device-level insight was quite important, saying "some device insight will help us better optimise costs and network resources".

Just 5% of respondents said they do not need to know what the traffic is, what devices are connecting to the network, or what behaviour said devices conduct while on the network, believing their organisation just needs to deliver rudimentary connectivity and nothing else.

Earlier in the report we identified enterprise use cases for IoT as one of the principal markets being targeted by operators, with a fairly sizeable proportion of the audience seeing it as an ideal revenue opportunity. Our next question asked the audience what level of importance they placed on the delivery of several enterprise IoT services. The generally high level of importance placed on most services in this question suggests the audience has reaffirmed its previous assertion that enterprise services in a variety of forms are a major opportunity for telecoms operators.

How important do you think it is to understand the specific identity, activity and requirements of each IoT device connecting to the mobile network?



Of a narrowly differentiated bunch, the three services most commonly identified by the audience as most important related to the need for elastic, agile and scalable service delivery to enterprise customers. Ranking as most important is the ability to activate services for customers on-demand, with 93% of respondents classifying it as either important or very important. 90% gave a high level importance to being able to prioritise specific device-generated traffic on their network. With 87%, being able to scale the amount of bandwidth required for services was seen as the fourth most important feature for enterprise IoT. The previous statistics corroborates general industry concerns over bandwidth availability and a general desire within the market to more intelligently control traffic types and make better use of available resources.

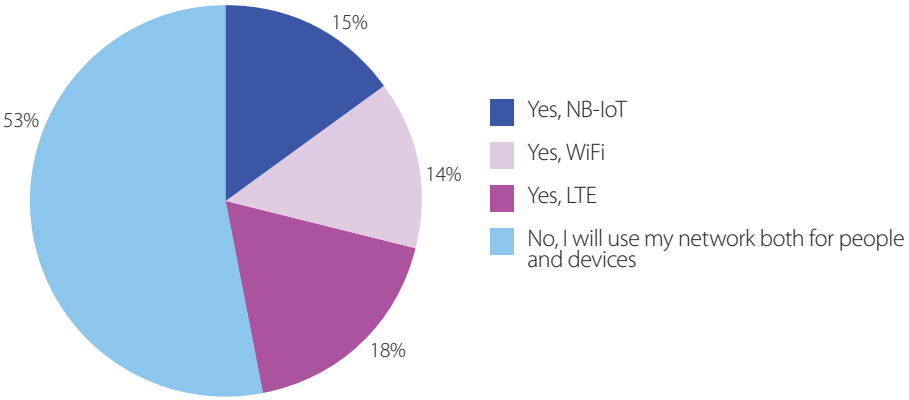
As well as looking to gain insight over the specific services users want to offer enterprise customers in an IoT context, we also sought to understand what the biggest enabling factors would be. Our question asked "how important do you believe the following factors to be in providing enterprise IoT services?" and the responses we received were ranked on a scale from very important to totally unimportant.

Telecoms.com readers said having the ability to monitor key performance indicators for devices on a global scale, with 93% rating it either important or very important. Having a dedicated connectivity or enablement platform also received an importance rating of 90% by respondents, which reflects the various attitudes we saw in the previous section of this report, with the audience noticing an intrinsic need to have an outsourced, cloud-based IoT management platform. 89% said they think it's important to have a broad array of IoT services available for enterprise – indicative of attitudes towards IoT's future ubiquity as a source of revenue generation.

IoT isn't going to be a purely localised set of services for domestic use, however, and international device and M2M roaming is likely to factor as a major consideration for

OPTIMISING IOT CONNECTIVITY

With the risk of fraudulent activity continuing to be a major concern, a more stringent level of standardisation, regulation and more cooperation between the industry are potential means for combatting the fraudsters.



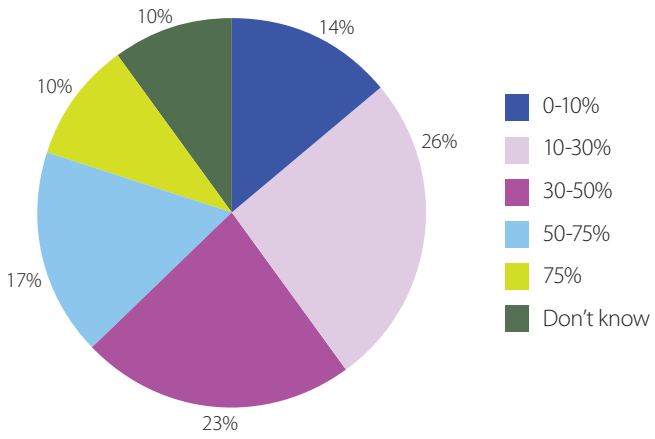
Do you plan on rolling out an additional dedicated IoT radio network in the near future?

operators and IoT-ready service providers looking to capitalise on the trend. 90% of respondents said inbound M2M traffic monitoring is going to be an important factor when considering the implementation of services ready for multi-national organisations.

With IoT roaming entering the discussion, our next set of questions posed a variety of scenarios for respondents to consider and rank in terms of the level of challenge they present. Deemed to be the most challenging was device fraud, identified by 90% of respondents as challenging or very challenging. Fraud within the telecoms industry is a perennial battle, and device or SIM-based fraud in recent years has led to significant revenue leakage on the operator side, and a negative experience in the eyes of the customer. Fraud in an IoT context will mean different things to different parties in the wider ecosystem, from charging malfunctions and to the leakage of sensitive information passing through various devices and systems. With the risk of fraudulent activity continuing to be a major concern, a more stringent level of standardisation, regulation and more cooperation between the industry are potential means for combatting the fraudsters.

On an international level, further concern is raised by devices which permanently roaming. With manufacturing a global business, embedded SIMs can be placed in various devices which are then shipped around the world, which once connected to a local network are registered as a roaming device, thus causing higher fees for the operator. One potential solution is to build intelligent identity swapping into each device, so that it appears as a local device on a foreign network. Regardless of the potential solutions, 88% of respondents deem permanent roaming a major challenge for them, and will require resolution. Other major challenges highlighted from this question cover malfunctioning devices and network signalling or data storm problems.

The operator network will, undoubtedly, bear the brunt for the majority of IoT traffic moving around; and as the penetration of mobile broadband and the broadening of its coverage continues, the radio access network will likely present the primary means of connectivity. With that in mind, just under half of the audience said they will be rolling out one of three dedicated, additional IoT radio networks in the near future to accommodate the rise in machine-based traffic. Of the three technology options presented, there was a relatively even split in the votes, with 18% saying they will be launching a dedicated LTE network, 15% saying the same for NB-IoT and 14% saying the same for Wi-Fi. There is the added option of not rolling



What percentage of IoT-generated traffic do you think will be processed by the mobile radio access network?

out an additional radio network dedicated to IoT, and 53% said they intend to use existing infrastructures for both people and devices.

The reason why more than half of the audience adopted such a mind-set is perhaps evidenced in the responses to the following question, where we asked what percentage of IoT-generated traffic will be processed by the RAN. In response to this question, the audience generally agreed that the RAN will not be responsible for carrying the majority of IoT traffic. 14% of respondents said less than one tenth of traffic will be processed on the mobile network, while just over one quarter believe it will accommodate 10-30% of IoT traffic. An additional 23% reckon between 30-50% will be processed on the RAN, and 27% think it will be more than half. 10% did not know.

So from this statistic we can conclude a general acceptance from the audience that the mobile network will not bear the brunt of the IoT revolution, but will still play a significant role in processing a fair amount of the generated traffic. The mobile network is in a perennial state of transition though, with LTE moving to LTE-A and, moving past LTE-A Pro, on to 5G the goal posts are constantly moving. Challenges are constantly evolving and our audience reckons getting the adequate analytics systems in place to accommodate the varying nature of IoT traffic is the biggest challenge operators will face – 90% deemed to be challenging or very challenging. Elsewhere, ensuring QoS, increasing profit and creating a streamlined and easily configured management platform for IoT ranked highly on the list of concerns – receiving 89%, 88% and 87% respectively.

Our final question in this section of the survey posted a straightforward conundrum to respondents. Do they believe current cellular networks are ready to fully support IoT? 14% said they didn't know, but of the remaining 86% that answered, just 26% reckoned today's mobile network is capable of dealing with the stresses and strains the next generation of connected things will create; meaning 60% do not think current cellular networks are up to scratch.

The mobile network will not bear the brunt of the IoT revolution, but will still play a significant role in processing a fair amount of the generated traffic.

Sponsor's Comment

Enterprise IoT services represent a huge market opportunity and growth potential for CSPs. The Telecoms.com readers clearly believe that service continuity is a major challenge when it comes to optimizing IoT connectivity and services. Survey respondents are clearly apprehensive when it comes to the CSP's ability to deliver a seamless solution that includes connectivity, visibility, control and security. 60% of readers do not believe that current cellular networks are ready to fully support IoT.

The overwhelming majority of the audience concurs that CSPs must be able to ensure seamless connectivity services; 88% say it is important that their CSPs implement systematic mechanisms to identify, prevent, predict and alert customers to avoid service disruption in areas such as resource optimization, security and fraud. Starhome Mach's HD-IoT platform provides a comprehensive Service Continuity and Security Solution for IoT connectivity.

Ninety-five percent of survey respondents regard the ability to identify the activity and requirements of individual IoT devices as important. HD-IoT enables MNOs to monitor traffic, analyse behavior, identify device types (domestic, inbound, outbound and localised) and detect any QoS issues. In addition, HD-IoT ensures uninterrupted connectivity with real-time anti-fraud or usage control, hybrid steering and real-time connectivity re-initiation.

Starhome Mach's service continuity solutions enable cooperation between roaming and IoT business stakeholders by adapting steering methods and behavior to specific device types and needs. Network connectivity can be streamlined by virtualizing network and IT capabilities for seamless deployment.

Starhome Mach's HD-IoT platform not only provides the basic services, steering, virtualization and security required by MNOs, but it also addresses the more complex services required for the Service Continuity of Global IoT.

SECURING THE IOT

Key takeaways:

- Nearly two thirds of respondents believe IoT will present new and unique information security challenges.
- An additional two thirds thing IoT is more vulnerable to security leaks due to the volume of devices and traffic being generated.
- One in three respondents think they don't experience any DDoS attacks.

About F5:

F5 (NASDAQ: FFIV) provides solutions for an application world. F5 helps organizations seamlessly scale cloud, data center, telecommunications, and software defined networking (SDN) deployments to successfully deliver applications and services 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 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.

You can also follow @f5networks on Twitter or visit us on LinkedIn and Facebook for more information about F5, its partners, and technologies.

Secure the **perimeter**

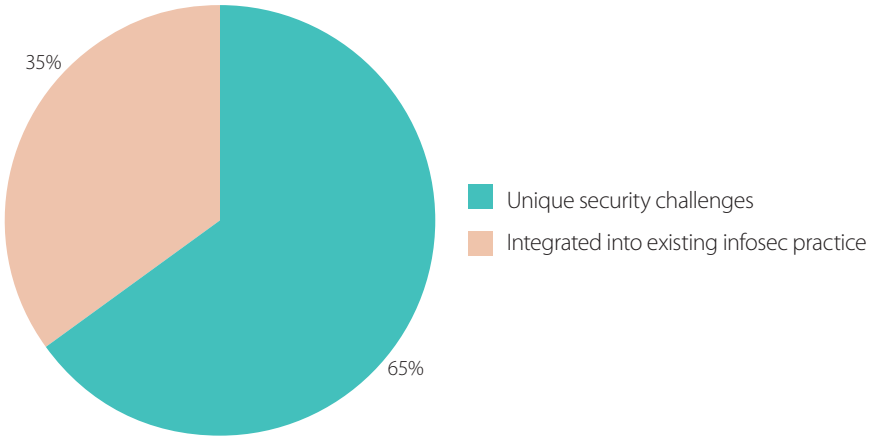
Security is firmly back on everyone's radar. Over the last couple of years media reports have broken with alarming regularity over various shortcomings, vulnerability exploitations, DDoS attacks or straightforward brute force hacks on the networks of major organisations the world over.

It wouldn't be too much an exaggeration to say that no company is 100% safe 100% of the time. The goalposts are constantly shifting as hackers and cyber criminals, either individually or in organised fashion, continually outwit or outpace the organisations they target.

While financial gain, politics, ideals or morality can be some strong motives for cybercrime – as was the case with the organised takedown of dating site Ashley Maddison last year – a lot of attacks can be completely arbitrary in nature. In a lot of cases, a victim isn't necessarily singled out due to any specific motive; it can often come down to a case of boredom on the hacker's part, or the accidental stumbling-upon of a particular vulnerability which can be exploited.

We have already established the sense of importance the respondents to this year's IoT Outlook survey have placed on security. The results of this section dedicated to security will explain and discuss various views and thoughts our audience has on how vulnerable the Internet of Things is to exploitation and targeting of specific attacks; the significance of various security challenges to the wellbeing of IoT; and how they plan to combat the risk.

To begin with, we asked the audience how vulnerable they think IoT is to malicious attacks, and gave three options to choose from. In the majority of responses from the audience, more than two thirds no less, 67% said IoT is more vulnerable than existing services due to the sheer number of devices and connections being formed on the network. While 29% of the audience believe IoT has the same level of vulnerability as standard broadband or mobile services. Just 4% believe IoT is less vulnerable than existing services due to the comparably smaller size of traffic being transmitted.



Will IoT present new and unique security scenarios, or will it be a natural evolution of existing information security practices?

So it has been established that the vast majority of the audience sees an equal or greater security threat to operator networks as a result of connected devices and the broader IoT, therefore what does the audience consider to be the most significant individual threat to their network?

While all answers were generally received with a high level of concern, the answers with the highest level of attention were somewhat related to the user-end side of the IoT stack. Security on individual devices received a security significance rating of 96% (seen as either significant or very significant), while gateway or router security issues received a rating of 94%. Additional concerns that ranked highly relate to the need to prevent DDoS attacks on IoT service components (93%), and the protection of cloud and data centre infrastructure (93% also).

With a variety of security concerns already established, we asked the audience whether the previously identified threats and the level of vulnerability of IoT security meant we will be presented with new and unique security scenarios, or if it will be a natural evolution of existing information security practises. Results suggested there will be a need for a dedicated IoT security strategy, as 65% said it will present unique security challenges for operators, while 35% believe they can integrate IoT into their existing information security practice.

As with any discussion surrounding a field as convoluted or perpetually evolving as securing an emerging technological principal, education and knowledge are key. Therefore, we sought to understand whether users felt security vendors have sufficiently addressed IoT security risk mitigation; and while the results yielded were not starkly polarising, they did suggest a clear need for more learning among the majority of respondents. 44% said the full challenge hasn't yet been fully explained and they are still learning about IoT

UK multiplay challenger operator TalkTalk is still reeling from the sustained and penetrative DDoS attack it suffered in October last year.

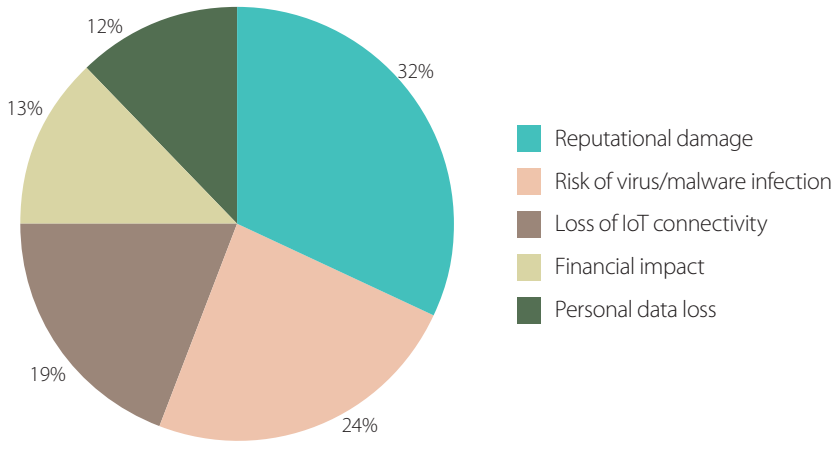
security. A further 28% said there's a need for maturation of technology and vendor offerings, with the user fully aware of what they require from an IoT security solution. 22% believe they will never know the true extent of all the threats to IoT security and can only do their best to keep up, while just 6% say they have already analysed and understood the security challenge and are in the process of implementation.

UK multiplay challenger operator TalkTalk is still reeling from the sustained and penetrative DDoS attack it suffered in October last year. At its recent year-end financial results, CEO Dido Harding revealed the financial impact the attack had on the operator; its profits dropped 50% year-on-year and its exceptional item expenses more than doubled in the same period, likely as a result of regulatory fines, consumer compensation, network forensics investigations, and the subsequent implementation of additional security measures.

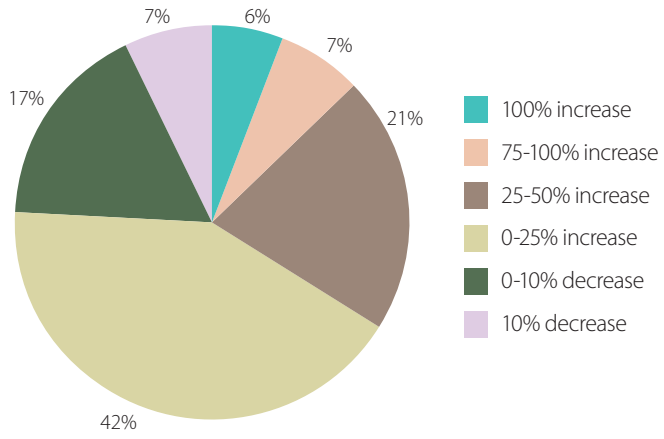
The case of TalkTalk is one close to home for telecoms service providers, and so we asked the audience how often they have to manage and mitigate attempted DDoS attacks on a monthly basis. Exactly one in three respondents said they never experience DDoS attacks, or attempted attacks on their network, which seems surprisingly high.

Of the remaining 66% of respondents, 27% say they experience one attack every month, 25% believe they're managing two to four attacks every month and just 6% say they are attacked between five to ten times every month. Alarmingly, nearly 10% of all respondents say they are attacked by DDoS more than ten times on a monthly basis, which implies a high level of resilience, and a successful and sophisticated information security infrastructure is in place.

With two thirds of the audience admitting they are managing with at least one DDoS attack every month, our thoughts turn to the potential repercussions if one of those attacks were to be successful. With the aforementioned cases of TalkTalk and Ashley Maddison making global headlines following a breach, as well as other cases including the likes of Sony, organisations are acutely aware of and even afraid of the reputational damage that can occur. In this case, 32% of our readers deemed this the biggest risk associated with a network or data breach in IoT. With negative reputational consequences comes distrust from users, and therefore a potential rise in churn and downturn in financial fortune. Elsewhere, a further 24% of the respondents said they are most concerned about the infection of additional malware and the risk of further viruses; 19% consider the loss of connectivity as the biggest risk factor; while 13% and 12% of the audience were most concerned about the financial impact and the personal data loss attributed with an attack.



What is the biggest cost to your business as a result of an IoT-related DDoS attack?



Year on year, how has your spend on IoT and network devices security changed?

When specifically considering the IoT use cases and IoT-generated network traffic, we asked respondents to select the statement that most accurately represented their point of view. 32% said IoT applications might introduce new security risks or invite DDoS attacks to the existing network and infrastructure – which in turn might impact other services on the network. 31% believe IoT applications might behave in unexpected ways and could potentially bring down elements of a dedicated IoT infrastructure. 26% said the risk of external attacks means there's a strong need for robust security policy at the perimeter of the network. 48% agreed strongly with all of the previous statements.

With security apparently presenting such a clear and present danger to the respondents of this survey, it therefore seems surprising that nearly a quarter of the audience are actively decreasing their spend on IoT and network device security year-on-year. 17% have made a 0-10% reduction, while 7% of respondents said they reduction in spend is greater than 10%.

The majority of respondents, however, are planning a 0-25% increase in security spend – with 42% being a statistic more in line with the general mentality seen in previous answers of this section. Furthermore 21% of the audience intends to invest 25-50% more on security than it did last year. 13% in total are planning on increasing their year on year security spend for IoT by more than 75%.

To conclude, we asked the audience a straightforward question: are you ready to offer a fully secured IoT offering? While half of the audience said they plan on doing so by 2020 at the very latest, 36% simply responded by saying no. The question saw just 15% of respondents say yes.

What we've seen from this section further compounded the assertion we established in the opening section of this survey: the vast majority of respondents see security as the single biggest threat to the success of IoT. The stakes are high, the threats and risks are unrelenting and constantly evolving, and while a certain level of the audience feels they're on the path to assuring their networks from would-be wrong-doers, there is an equal portion of the industry which feels they'll simply never be able to keep up with the threats.

Sponsor's Comment

Industry projections estimate that there will be 50 billion connected devices worldwide by 2020, or 7 devices for every person on earth. To handle this explosive growth in the number of devices and applications, service providers (SPs) believe that they will face tremendous pressure to build networks that are secure and scalable.

From the Telecom.com Intelligence IoT Outlook 2016 report, SPs believe that the increased number of applications and services will open up new and unknown threat vectors that could expose their assets, impact service availability, and most importantly, damaging their reputations and brands.

SPs believe that IoT will introduce new and unique challenges. The large and diverse number of devices connected to the network could become targets of hacking and denial-of-service attacks. The full challenges haven't been fully understood, and SPs are still learning about IoT security requirements. An overwhelming 67% of SPs surveyed saw that their network experienced Distributed Denial of Service (DDoS) attack at least once a month. These damaging effects from DDoS attacks and malicious Advanced Persistent Threats (APTs) against networks could have severe consequences. These evolving threats put tremendous pressure on service providers to build and strengthen security in the network. At least 25% or more of the SPs surveyed expect security spend to increase year-over-year.

Aside from security, scale and performance will also be required to handle the surge of millions to billions of secure DNS requests per second that may impact network performance and availability. The inevitable spikes in network signaling, and attacks in signaling protocols such as SIP and Diameter, could cause signaling storms, potentially bringing down the network.

To optimise performance and improve quality of user experience, SPs will additionally need tools to manage traffic priority and steer traffic based on the device type, application, and associated signaling.

To protect against sophisticated and emerging threats, and maintaining a highly available network, SPs will need to secure every layer in their network. This includes protecting the network and applications from known and unknown security threats that impact devices, networks, and applications. SPs will need comprehensive security solutions to ensure and protect user data and networks at every layer. This includes mitigating and protecting attacks on the DNS infrastructure, core network resources, and L7 application services.

INDUSTRIAL IOT

Key takeaways:

- Nearly half the audience says professional enterprise services and analytics software will be the biggest revenue generator for industrial IoT.
- 81% believe telecoms operators will face threats from new market entrants as a result of IoT pervasion.
- Just over a quarter of respondents feel conflicting standards will inhibit industrial IoT's potential.

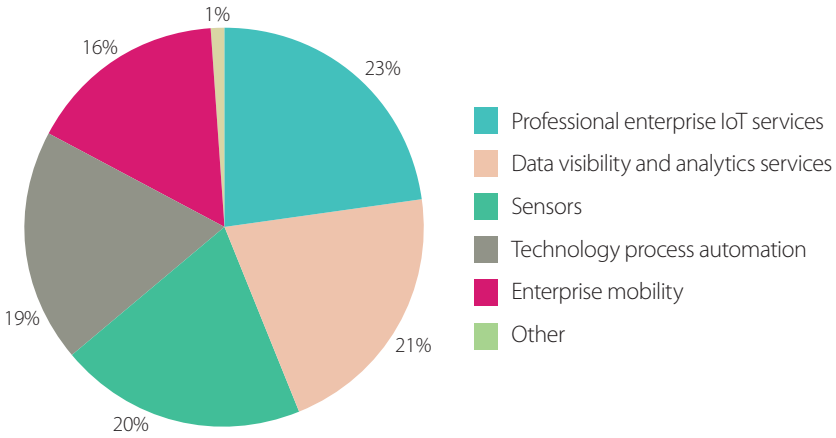
An **industrial** approach to things

As we've already seen earlier in this report, a sizeable percentage of the audience believes industrial IoT (IIoT) and use cases for enterprise customers remains one of the primary monetisation opportunities for operators.

In this sense, industrial IoT could span a range of market sectors including anything from utilities to oil and gas, to enterprise organisations and retail. To dive further into what the audience believes could be a potential winner for enterprise/B2B IoT, we asked a range of questions about how the operator is positioned to deliver carrier-grade industrial IoT, what the biggest opportunities and challenges are, and also what the role of the telco will likely be in this subsection of the industry.

We began by looking to establish where the audience is today in terms of enterprise-ready IoT applications or services. More than a third (35%) of the audience says they are currently providing services today – which is nearly double the number of respondents who were actively commercialising IoT in 2015's survey. This doubling of live use-cases suggests, principally, that IoT is gaining significant real-world traction and coming much closer to fruition than it had been 12 months previous. While it is still reasonable to suggest these IoT services are relatively rudimentary by nature, it is not inconceivable for them to rapidly evolve as an increasing percentage of the industry gets to grips with IoT and begin draining it for its fullest potential.

With use cases on the rise, we wanted to understand which elements of IoT in the enterprise appeals most, and which services will be the biggest revenue generator for operators. The most commonly identified by the audience in this regard is the delivery of professional, enterprise-grade IoT services, which received 23% of the votes. Harking back to the trend previously established in the report, analytics and data visibility services also gained significant traction the audience and 21% deemed this type of software to have the most revenue generation potential. Of the remaining possible answers to this question, respondents saw physical IoT hardware as having the biggest potential for revenue generation, as one in five suggested the sheer volume of sensors associated with making IoT possible will present a sizeable financial opportunity. Elsewhere, technology process automation and enterprise mobility services gained 19% and 16% of the votes respectively.

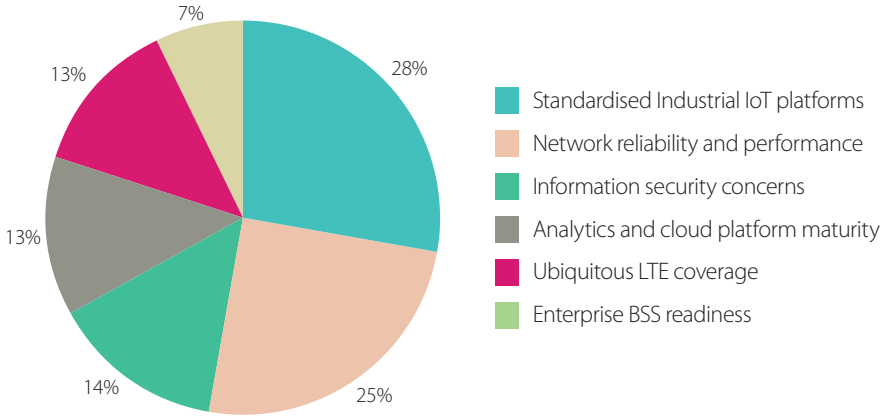


Which of the following do you believe will be the biggest revenue generating services for Industrial IoT?

Financial gains aside, we also asked the audience to share their views on which two elements of industrial IoT will present the biggest benefit for businesses. The two most commonly selected answers to this question revolved around process improvements, as 39% voted for operational efficiency gains, with a further 35% saying business process automation will be the biggest benefit. 26% of the audience stated that using IoT to generate enhanced IT insight and analytics capabilities, while another 26% voted for predictive maintenance as a result of aforementioned analysis tools. Just 8% of the audience opted for research & development gains as a result of utilising enterprise-ready IoT services.

With several bases covered regarding the benefits and capabilities of industrial IoT, the operator is widely regarded as the glue holding the whole thing together. With that in mind, the next set of questions presented a variety of statements regarding the role of the telecoms operator in the development and delivery of IIoT services. Respondents were asked to rank each statement on a scale of Strongly Agree to Strongly Disagree, and the results were aggregated to yield an average agreement rating.

The overarching theme emanating



As a telecoms service provider, what do you think will be the biggest barrier to Industrial IoT implementation and success?

"There is both work to be done and a competitive threat from market entrants in a new digital landscape facilitated by IoT."

from the results suggest operators are generally well positioned to deliver IoT services for enterprise or industrial purposes as things stand today, although there is both work to be done and a competitive threat from market entrants in a new digital landscape facilitated by IoT, a statement which was agreed (or strongly agreed) with by 81% of the audience. Lowered barrier to entry notwithstanding, 80% of the audience sided with the telco and said operators are in the best position to provide enterprise organisations with IoT-based services. In consideration of the networking requirements of delivering industrial IoT, 70% of the audience agree that telcos can only begin monetisation of IoT after deploying a comprehensive LTE mobile network for IP traffic. Meanwhile, the most heavily disagreed with answer stated "Industrial IoT will only become valuable for operators once 5G arrives", a notion which nearly half of respondents rejected.

The penultimate question in the section asked operator respondents to identify which challenges will prove most prohibitive in the quest for IIoT success. The general consensus suggests a conflict exists between platforms for industrial IoT, and a lack of standardisation is the biggest barrier – identified by 28% of the audience. Anxieties over network performance also feature highly, with exactly a quarter of respondents highlighting reliability and speed. Incidentally, an additional 13% believe ubiquitous LTE coverage is the biggest challenge.

Meanwhile, information security concerns pulled in 14% of the audience's votes, while analytics and cloud platform immaturity also gained a further 13%.

The final question in our section seeking clarity surrounding industrial IoT asked questions to identify one statement which most accurately reflected their attitude towards, and the findings back up our earlier assertion that internal business optimisation is the biggest driver.

Just over half of the audience said industrial IoT is mainly about improving asset and process efficiency, while 42% of respondents instead said it is more ideally suited to enabling the development of new and improved business services for enterprise customers. Just 7% of respondents to this question said industrial IoT is instead about minimising losses.

While it appears relatively conclusive that the audience sees a large amount of opportunity in the enterprise or industrial applications of IoT technology, there are a number of challenges associated with making it a tangible reality. Adding a variety of differing opinions on the most pressing issues and general air of confusion over standards and which platforms will bring the most benefit, we can conclude that despite its potential, more work needs to be done before the telecoms industry will consider enterprise-grade IoT to be here and flourishing.

CONSUMER IOT

Key takeaways:

- Nearly two thirds of the audience believe consumer-related profucts will be a major element of their IoT strategy.
- Just 7% of respondents think wearable tech will really take off.
- A completely driverless experience will be the biggest benefit of connected cars, according to 27% of the audience.

Driving **consumption**

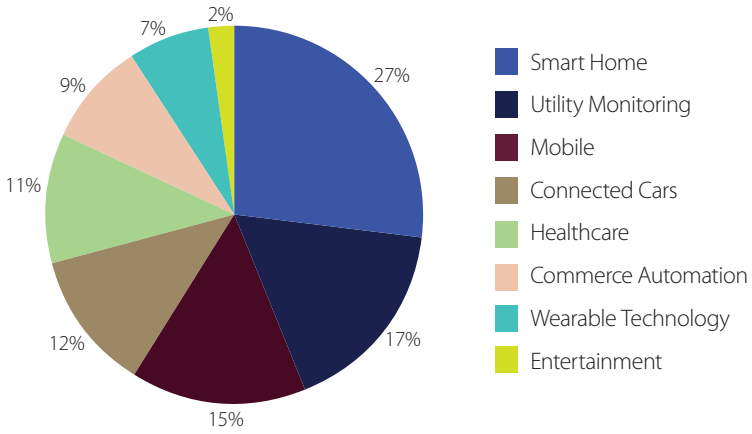
In the eyes of broader consumer media, IoT has been painted as the technology which will deliver on the quintessential utopian vision of a fully automated house. Cars will automatically drive us to work; fridges will talk to supermarkets; toasters will talk to kettles; and breakfasts will be made on time and to perfection.

This picture has been painted in the mainstream media or science fiction movies for decades, and has been brought substantially closer to reality by the gradual advent and introduction of IoT-based smart home gadgets and gizmos in recent years. The fully automated dream is still only really being taken up by the early adopters within the technology lifecycle theory, but momentum is beginning to gather, and the majority of the Telecoms.com audience still thinks of consumer related product offerings when asked what they primarily associate with IoT.

It isn't just in the 2016 version of the IoT Outlook where consumer offerings have risen up to be the most potentially positive IoT trend identified by the audience. In last year's edition more people voted for home automation and connected cars than any other as the most traditional IoT-ish use case; while a poll run on Telecoms.com saw devices and home automation each dominate the popularity rankings when asked a similar question.

With that in mind we sought to further understand how the audience views consumer-related offerings for IoT going forward. Perhaps unsurprisingly, when asked whether consumer product sets will provide one of the main IoT opportunities for their business, 63% of respondents said yes. While 13% said they didn't know, suggesting it is still too early to tell just yet, just under one quarter said consumer will not be one of the main IoT markets they plan on pursuing.

Reflecting on trends identified over the past year, where we saw consumer IoT as the most identified-with by our readers time and again, we asked which subsection of consumer IoT has the most potential. The most popular response by some distance



Which consumer IoT category do you believe has the most potential for your business?

suggested smart home technology is likely to be the most lucrative or game-changing opportunity for operators. Considering some facets of IoT in the home are well on the road to maturity and monetisation this year, including metering, security, surveillance and home automation, consumer IoT might be closer to reality than we previously realised.

Elsewhere, utility monitoring, mobile, connected cars and healthcare received comparatively favourable results from the audience, receiving 17%, 15%, 12% and 11% respectively.

The audience does not however, appear to hold out much hope for wearable technology. Despite global consumer electronics firms relentlessly reminding consumers just what they're missing out on by not buying a new smart watch, only 7% of the audience reckon wearable personal devices are going to have an impact on consumer IoT going forward.

Back to the smart home, though, and we used our next question to further clarify audience attitudes on its sustainability as a business model and how big an emphasis operator will be putting on it in the future. While roughly 40% say home automation either won't be a consideration at all, or are just yet to consider it, the remainder of respondents saw its business viability in much more favourable light. Just over one quarter of respondents say they are aiming to provide monthly, billable services of varying degrees to enable home automation. Additionally, more than one third of respondents are going big on home automation, with 34% saying they will be providing a full suite of home automation services which will become integrated into future consumer-facing connectivity offerings.

Our next question focussed on using mobile apps as a means of interfacing and controlling smart home services. Here, we provided respondents with a variety of statements and asked them to state their level of agreement, on a scale of "strongly agree" to "strongly disagree". The general consensus from the set of statements put forward suggests consumer IoT is only as effective and successful as the user experience of companion mobile apps – 92% either agreed or strongly agreed. We also saw 88% of the audience agree that a companion app is absolutely essential for all consumer-based IoT products; conversely, 86% of the audience simultaneously agreed that even if a product doesn't strictly need an application, consumers will still expect well-designed companion apps with their products. Another 86% said that app aesthetics is surprisingly important for the future of IoT, agreeing that "if an app doesn't look good or integrate seamlessly, consumers will reject IoT as part of their daily lives".

The statement receiving the least agreement, and by extension the most disagreement, said applications aren't necessary for the majority of consumer IoT products and simple connectivity is ample for the best part. This reinforces the belief that the interactive experience through the use of mobile-based applications is an essential factor in determining the success of IoT in the everyday lives of consumers.

The final element of this consumer-focussed section of the 2016 IoT Outlook put connected cars in the headlights. The automotive industry has frequently been flagged up as one of the sectors where IoT could have its biggest impact. The concept of having a connected vehicle relaying performance metrics, driver assistance, in-car entertainment or even total driving automation has gained significant traction, investment and excitement from many quarters. Giant technology firms such as Google, Apple, Tesla and the likes have been piling cash and resources into forward-facing ventures in the hope that taking IoT to the road will pay off in the not-too-distant future.

With the imminent evolution of the driving experience seemingly looming large, we sought to understand which facet of automotive connectivity respondents to the survey deemed the most viable, and what form of connected cars will likely take off.

Exactly half of the audience believe the connected car will be a hybrid of real-time information being beamed into the vehicle and driver assistance, features like traffic updates and performance monitoring for example. A further 27% believe IoT for cars will manifest in the form of total driving autonomy – saying the connected car will be a driverless experience facilitated by the arrival of 5G. Indeed, one of the much touted features of 5G will be its ability to deliver and transmit data with sub-1 millisecond latency. The biggest challenge in delivering an automated driver will be this latency performance, along with the 100% reliability and resiliency – not to mention the hurdle of allaying societal fears of putting their safety and wellbeing into the hands of a machine.

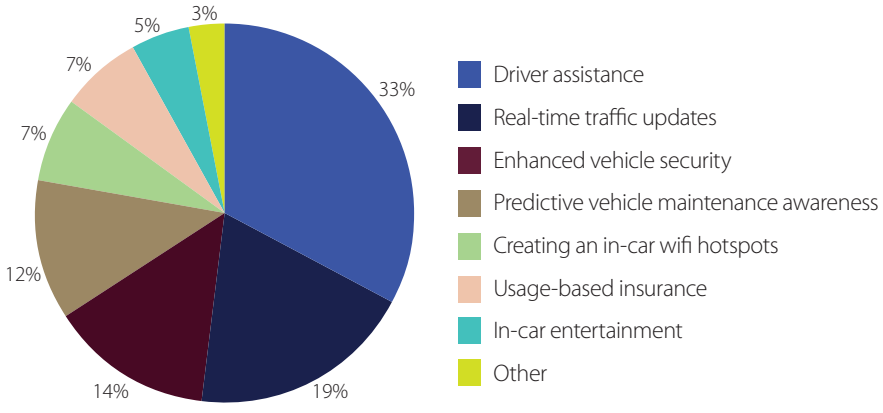
Incidentally, 23% of respondents said the connected car is overhyped and will not be playing a major role in future IoT strategies.

The final question of this section, and the survey, asked respondents which feature of connected cars will prove to be the most beneficial. While the audience appeared indifferent towards in-car entertainment, usage-based insurance and in-car wifi hotspotting – gaining 5%, 7% and 7% of votes respectively – performance-related features did gain significant traction.

Exactly one third of voters said driver assistance, which includes automation and real-time notifications, was the biggest benefit of connected cars. Real-time traffic updates was the second most popular with 19%, with enhanced security and predictive vehicle maintenance awareness getting 14% and 12% of the votes respectively.

In summary, it would appear the majority of the audience is looking forward to pushing ahead with consumer-related IoT offerings, and holds out hopes for its future potential. Major challenges exist in delivering compelling products with a stable and aesthetically pleasing interface for an increasingly fickle consumer base. Positivity over home automation solutions as a future revenue stream is tempered by a relative indifference towards connected cars, inferring further development and definition of a winning consumer-IoT strategy is still required.

"Giant technology firms such as Google, Apple, Tesla and the likes have been piling cash and resources into forward-facing ventures in the hope that taking IoT to the road will pay off."



What do you consider to be the biggest benefit of connected cars?

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