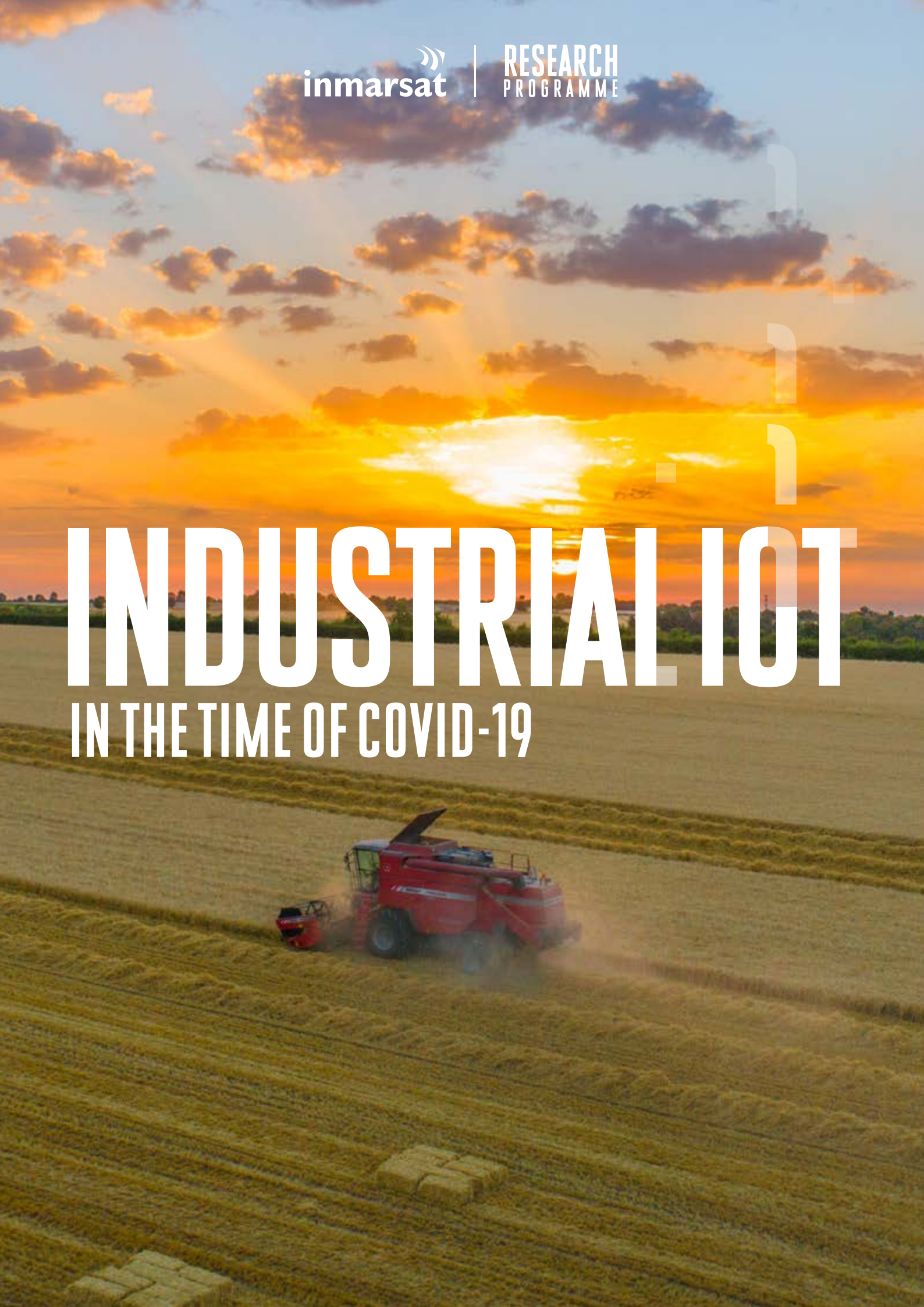
inmarsat | RESEARCH PROGRAMME

INDUSTRIAL ICT

IN THE TIME OF COVID-19



ABOUT INMARSAT

Inmarsat is the leading provider of global mobile satellite communications services. Since 1979, Inmarsat has been providing reliable voice and high-speed data communications to governments, enterprises and other organisations, with a range of services that can be used on land, at sea or in the air. Inmarsat operates around the world, with a presence in the major ports and centres of commerce on every continent. For more information, please visit **www.inmarsat.com**

CONTENTS

METHODOLOGY

The Inmarsat Research Programme is now in its fifth year, with this 2021 report providing an update on how the industrial Internet of Things (IoT) is being adopted by organisations across the agriculture, electrical utilities, mining, oil and gas and transport and logistics sectors.

Specifically, this report looks at the impact of Covid-19 on IoT adoption, as well as challenges related to connectivity, skills, security, data and investment.

To understand this Inmarsat commissioned Vanson Bourne, a specialist technology market research company, to interview 450 respondents in early 2021, a year after the start of the pandemic.

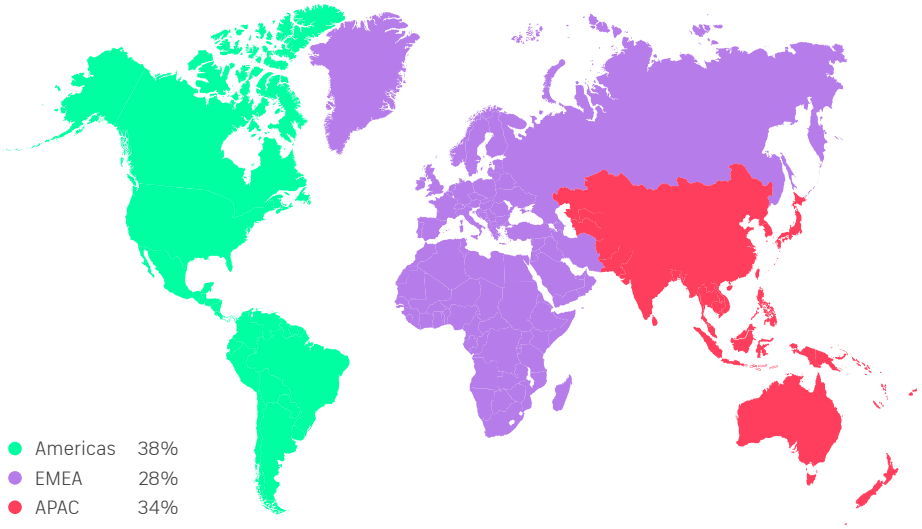
Respondents work for organisations with at least 250 employees and are drawn from various global regions including the Americas, EMEA and Asia-Pacific. All of those surveyed are responsible for delivering IoT initiatives at their respective organisations.

HOW MATURE IS IOT AT YOUR ORGANISATION?

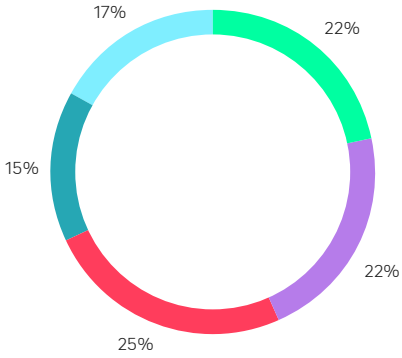
Inmarsat's free IoT maturity tool helps you compare your organisation's IoT maturity with our respondents and your competitors. Your personalised report also explains what you need to do to improve your score.

www.inmarsat.com/iotmaturitytool

Respondents by region

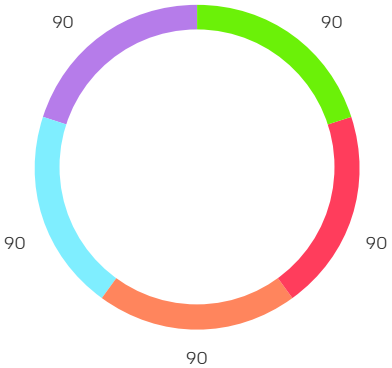


- Americas 38%
- EMEA 28%
- APAC 34%



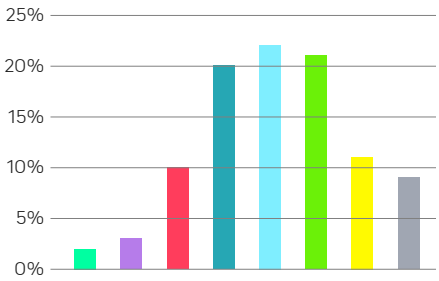
Respondents by size of organisation

- 250 - 500 employees
- 501 - 1,000 employees
- 1,001 - 3,000 employees
- 3,000 - 5,000 employees
- More than 5,000 employees



Respondents by sector

- Agriculture
- Electrical utilities
- Mining
- Oil and gas
- Transport and logistics



Respondents by turnover

$1 million - $50 million	2%
$50 million - $100 million	3%
$100 million - $250 million	10%
$250 million - $500 million	20%
$500 million - $1 billion	22%
$1 billion - $5 billion	21%
$5 billion - $10 billion	11%
$10 billion and above	9%

EXECUTIVE SUMMARY

- **The world's production and supply chains are becoming increasingly interconnected and digitalised to increase efficiencies and overcome challenges such as climate change, feeding a growing population and supporting sustainable and ethical industry**

- **Covid-19 is a black swan event that has emphasised the importance of Industry 4.0 technologies like IoT, and those adopting IoT are those best placed to succeed**

- **While IoT has undergone increased adoption rates since 2018, partly due to Covid-19, there are still areas that must be optimised such as connectivity, skills, data, security and investment levels**

The Covid-19 pandemic has brought unprecedented change to a globalised world, both for consumers and the industrial production and supply chains that serve them. Fluctuations in demand and supply have challenged agricultural producers and miners, transport and logistics companies have had to work increasingly reactively to keep supply chains going, while energy producers in the oil and gas and electrical utilities markets have seen reductions in demand and challenges in supply as much of the world ground to a halt.

A year on and parts of the world economy have returned to something like pre-Covid levels, though this period will serve as a stark illustration of why business continuity planning and the digital technologies that underpin it are so critical. Those organisations that have come through this period best are those that have embraced digitalisation, accelerated their adoption of Industry 4.0 technologies and adapted their business models to give themselves the best chance of weathering the next twist of fate.

While the road to the end of the pandemic is unclear, other challenges that have been building over time still remain. The global population continues to swell, with consumers challenging organisations to produce more, and quicker, with finite resources. The ever-present backdrop of climate change is forcing businesses to consider their carbon footprint while their behaviour is governed by Environmental, Social and Governance (ESG) best-practice and regulation. Employee and community welfare is no longer an after-thought. Safety comes first, with companies increasingly adopting a Zero Harm policy.

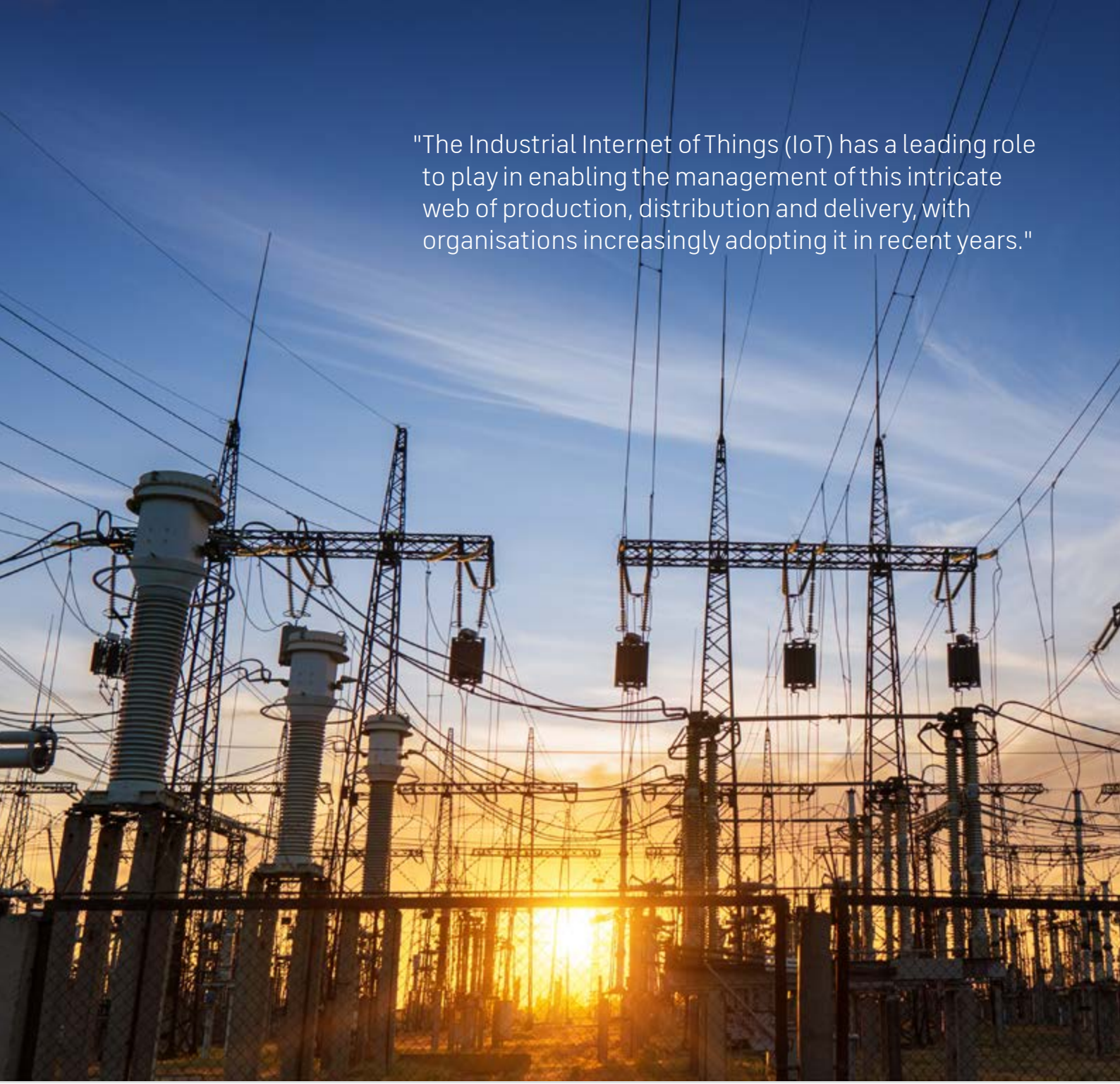
These forces are being felt across all of the increasingly interconnected industries that we examine in this report. Positive change is happening, enabled by technology that provides transparency and the ability to understand value chains in a way that was previously impossible. Now organisations are choosing to work with likeminded businesses, to collaborate and share data, to optimise operations and to show consumers provenance and their commitment to end-to-end sustainability and ethical business.

The Industrial Internet of Things (IoT) has a leading role to play in enabling the management of this intricate web of production, distribution and delivery, with organisations increasingly adopting it in recent years. Utilising an array of connected data producers to keep tabs on valuable assets, companies are producing 'digital twins' of their supply chains, so that each stage is recreated in digital form. Those companies leading the way with these projects, big and small, are the ones reaping the benefits of optimised operations and increasingly closer, more efficient partnerships with the organisations in their supply chain.

In living memory most businesses have moved their shop window online in the form of a website, those that have failed to move in step have likely fallen by the wayside. In the same way, businesses not digitalising their operations as part of the new connected supply chain model, will face significant challenges as these ways of working become ubiquitous. Increasingly, these smaller digital twins will combine to form an interconnected digital twin of all the world's supply chains, ushering in a new era of efficiency, safety and sustainability.

We find ourselves at a point, where like cloud before it, the term IoT has achieved ubiquity. This means that while an understanding of what IoT is, and its adoption is commonplace, there is a great amount of variation in the size, scope and potential outcomes of these projects. It also means there is a degree of variance in satisfaction and dissatisfaction as the technologies and skillsets, which underpin IoT, reach maturity.

Despite the increased speed of IoT adoption in recent years, there are a number of important areas identified in this report where organisations must still improve to draw the optimum benefits from the technology. Adoption levels are strong and companies are seeing significant return on their IoT investment, but connectivity and data strategies are not yet as advanced as they need to be. In a similar vein, businesses often do not have the



"The Industrial Internet of Things (IoT) has a leading role to play in enabling the management of this intricate web of production, distribution and delivery, with organisations increasingly adopting it in recent years."

skills needed to truly maximise the potential of IoT, particularly when it comes to security and analytical capabilities. The cyber-security vulnerabilities that IoT presents are also never far from the minds of our respondents and nor should they be, with bad actors looking to exploit an increase in connected things.

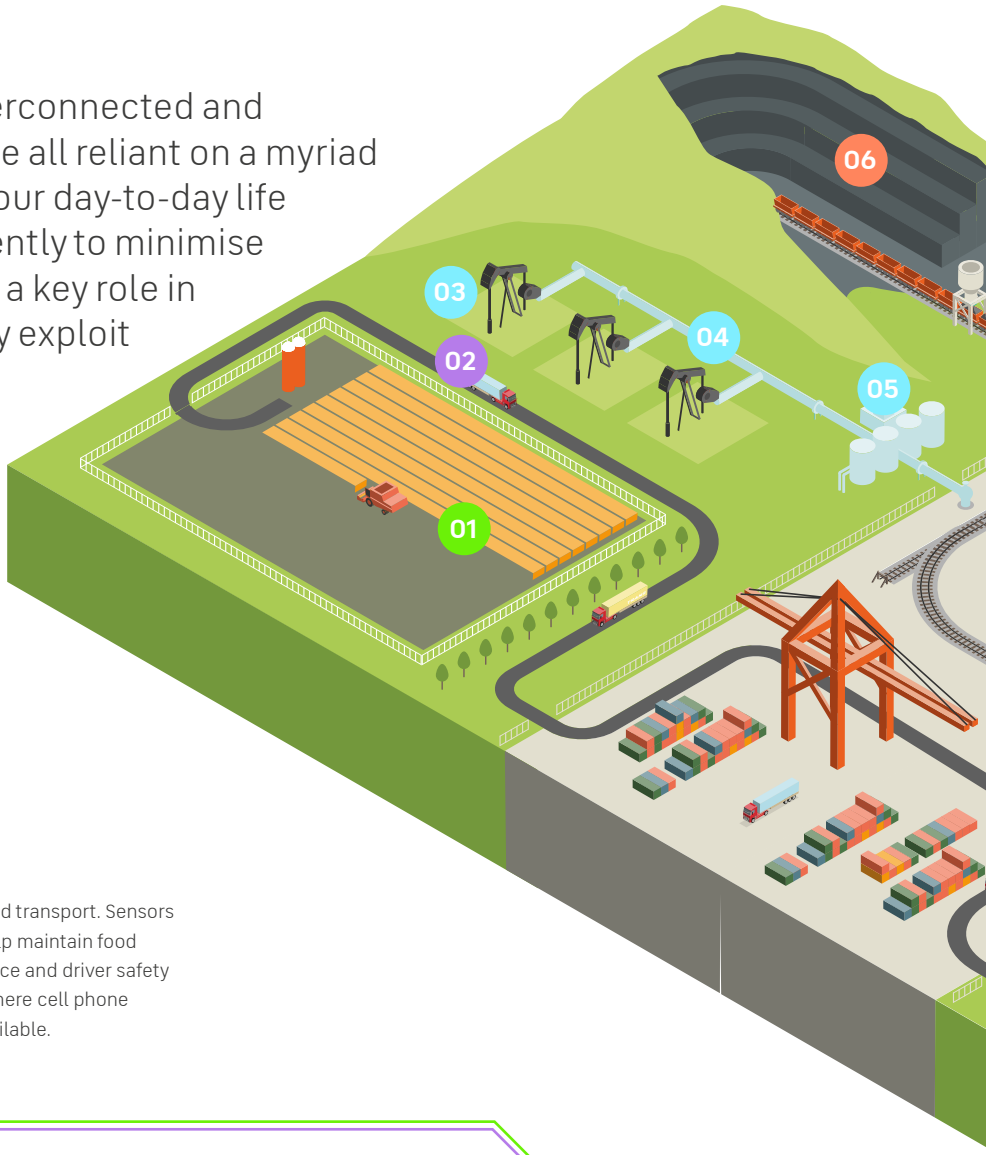
Reliable, flexible satellite communications is playing a key role in enabling IoT for businesses, allowing data to be collected, stored and analysed from anywhere on the planet, including far-flung sites well out of reach of terrestrial connectivity. From a remote farm in Brazil, a mining facility in Western Australia or an oil well in the Arabian Desert, there does not need to be a segment of a digital twin supply chain that is not visible. Businesses are increasingly appreciating that data collected in the remotest areas is often the most valuable, as business-critical activities are happening in these places.

Our research sheds light on the next steps organisations must take on their IoT journeys, in order to iron out any lingering issues, form better relationships with supply chain partners, and gain the skills needed to make IoT a success. We also look at what effect Covid-19 has had on IoT adoption during the period of the pandemic and what businesses might learn from this and implement in the longer-term. We invite you to also compare your business' relative IoT maturity versus those we have interviewed by using our IoT maturity tool here:

www.inmarsat.com/iotmaturitytool

GLOBAL SUPPLY CHAINS

The global supply chain is interconnected and increasingly digitalised. We are all reliant on a myriad of supporting value chains in our day-to-day life and all parts must work efficiently to minimise disruption. Satellite is playing a key role in helping global industry to fully exploit the possibilities of IoT.



CROPS
Field and crop health are monitored and maintained using localised sensors to provide insights on water and nutrients to make better decisions on the application of water and fertilizer to maximise yield.

TRUCKS
Food storage and transport. Sensors and tracking help maintain food safety compliance and driver safety even in areas where cell phone service is unavailable.

01 02

ON-SHORE RIGS
Upstream production – IoT delivers real-time process monitoring and predictive maintenance, as well as production levels, providing vitaldata on energy supply.

PIPELINE
Midstream transport – Sensors gather data to monitor for leaks and ensure environmental protections are maintained. Flow meters ensure production is controlled and improves accountability of different operators at hand-off points.

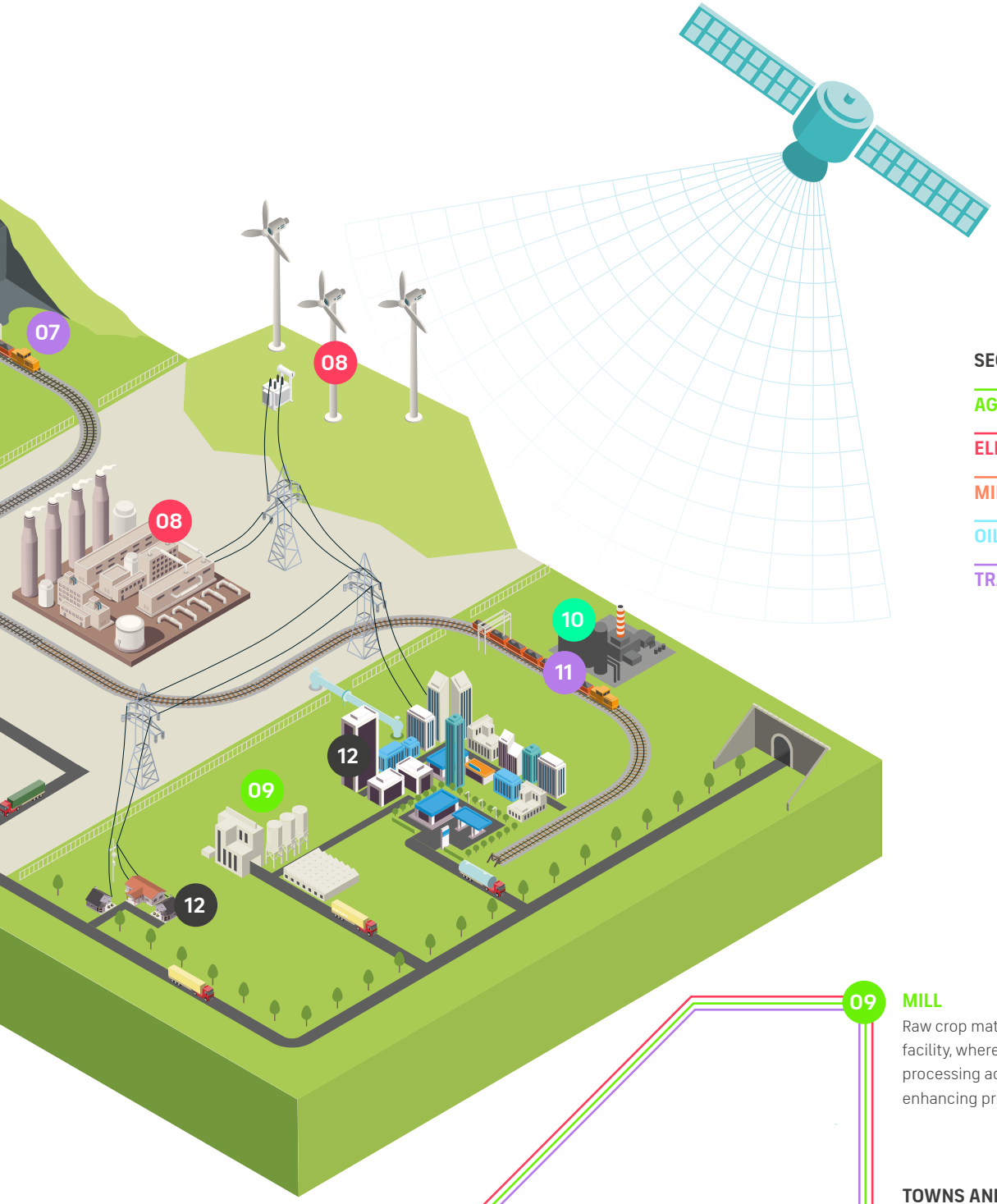
REFINERY
Crude oil processing – Analyses data received from pipeline and production equipment upstream to optimise refining process, integrated sensors inform transport partners in real-time of expected product quantities.

03 04 05

MINE
Mineral extraction – Connected sensors ensure efficient and profitable extraction, improving sustainability and staff health and safety.

AUTONOMOUS RAILWAY
Material transport – IoT enables autonomous railways to reduce transport costs and monitors cargo loads, providing critical transparency over supply chain.

06 07



SECTORS

AGRICULTURE

ELECTRICAL UTILITIES

MINING

OIL AND GAS

TRANSPORT AND LOGISTICS

09 MILL

Raw crop materials is transported to a mill facility, where sensors integrated into processing accelerate production, enhancing profitability.

TOWNS AND CITIES

Tracking and status monitoring during transport ensure efficient supply chains get the right materials and goods to the right customers at the right time. IoT also helps ensure end-to-end traceability to ensure corporate social responsibilities are met.

11 FREIGHT TRAIN

Steel is transported from smelting facility to urban hubs via freight rail networks, with IoT connected sensors providing real-time asset tracking data and improving security through detecting efforts to tamper with cargo.

08 ELECTRICITY SUPPLY

Energy producers and distributors rely on IoT to provide visibility and control across their grid infrastructure, ensuring electricity supports consumers and industry in remote and urban locations.

SMELTING PLANT

IOres are transported to smelting facility, where IoT connected sensors can improve the efficiency of the roasting and reducing process to accelerate steel production, and improve staff health and safety to ensure a safer working environment.

EMERGING TRENDS

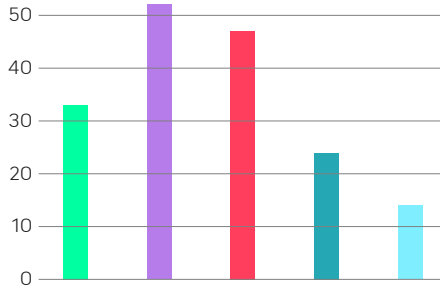
To understand IoT maturity, we look at a number of key areas such as adoption, connectivity, data, skills, security and investment. While we delve deeper into each sector's specific trends later in the report, examining the interconnected industries of the global supply chain as a whole provides us with a view on its overall health and the areas where organisations need to work together toward further improvement.

ADOPTION

IoT adoption has seen huge progress in the last few years, with 77 per cent of respondents having fully deployed at least one IoT project. This is an increase from just 21 per cent in our 2018 survey. Of the remaining 23 per cent that have not yet adopted IoT in any form, all of them are either currently trialling it, or plan to deploy or trial at least one IoT project in the next 18 months.

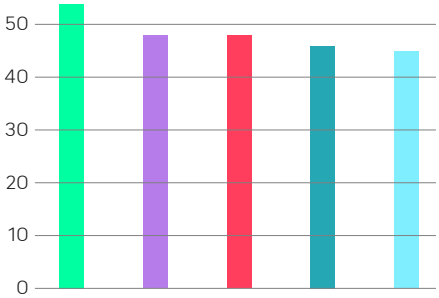
An interesting result of the Covid-19 pandemic has been to supercharge the adoption of IoT, with much of the IoT adoption occurring since the start of the pandemic in 2020, and many organisations stating they have accelerated their IoT projects in response to Covid-19. This can be attributed to IoT's remote monitoring and control capabilities, which enable operational continuity even while the movement of people is reduced. Those companies that have already accelerated their IoT deployments or who have IoT strategies are demonstrating greater levels of business continuity and the ability to weather the Covid-storm.

The drivers for IoT adoption are diverse, covering areas such as cost efficiencies, better environmental sustainability, better supply chain insight, greater automation and better decision making. It is clear from this that organisations have gained a good degree of awareness around the benefits that IoT can provide and are eager to embrace it; the next step is to fully optimise the deployments they have in place.



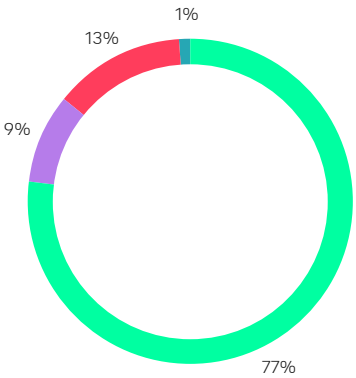
Covid-19's impact on IoT adoption

- Covid-19 has negatively influenced our ability to operate 33%
- Challenges related to Covid-19 have underlined the importance of IoT 52%
- We have accelerated deployment of IoT projects in response to Covid-19 47%
- We intend to accelerate our deployment of IoT projects in next 12 months in response to Covid-19 24%
- We intend to accelerate our deployment of IoT projects beyond 12 months in response to Covid-19 14%



The top 5 drivers of IoT adoption

- Cost efficiencies 54%
- Environmental sustainability 48%
- Better supply chain insight 48%
- Greater automation 46%
- Better decision making 45%



What is your current status when it comes to deploying IoT projects?

- Fully deployed
- Currently trialling
- Planning to trial within 12 months
- Planning to trial in 18 months – 2 years

77%

of respondents have fully deployed at least one IoT project

CONNECTIVITY

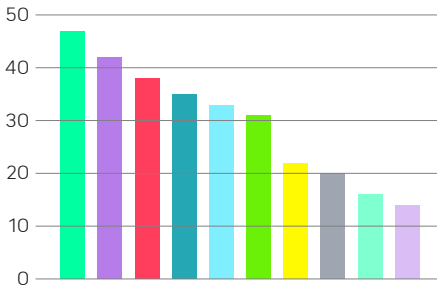
IoT is a network of networks and the success of IoT projects hinges on connectivity being reliable, available and responsive enough to deliver actionable data at the right time and the right cost to deliver strong return on investment. 75 per cent of respondents struggled to deploy their IoT projects because of issues with their connectivity types, demonstrating the value of reliable connectivity.

The suitability of connectivity types will vary depending on the goal of the project and often multiple types will be used together in one project. A project might include edge connectivities like LoRaWAN combined with backhaul connectivity types like satellite or cellular carrying data from the edge to a data centre or platform.

Satellite ranked as the most prominently used long range technology, while Wi-Fi is most common from a short-range perspective, reflecting Wi-Fi's low-cost point and flexibility of data type, versus more specialised edge connectivity types. The combination of different connectivity types suggests a more mature approach to IoT – so long as they are being used efficiently – with the average number of connectivity types used across an organisation being three.

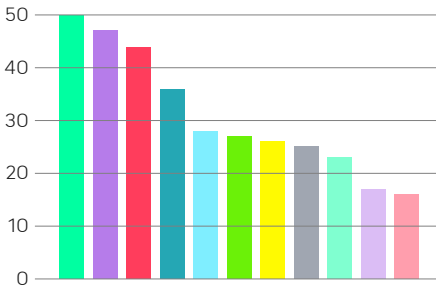
Encouragingly, when our respondents were asked what qualities they most desired in their IoT connectivity, respondents opted for reliability as their top requirement, with security in second and network coverage in third. Bandwidth and cost were lower priorities, suggesting respondents are aware that wide bandwidth is not always necessary for IoT projects where small packets of data are being transferred.

"75 per cent of respondents struggled to deploy their IoT projects because of issues with their connectivity types demonstrating the value of reliable connectivity."



What are the key considerations when choosing connectivity types for IoT where terrestrial connectivity is lacking?

Reliability	47%
Security	42%
Network coverage	38%
Bandwidth/speed	35%
Cost	33%
Latency	31%
Integration with existing tech	22%
Scalability	20%
Mobility	16%
Third-party support	14%



What connectivity types do you use in your IoT projects?

Wi-Fi	50%
Satellite	47%
Radio	44%
Cellular/LTE (public)	36%
Fibre	28%
Cellular/LTE (private)	27%
Bluetooth Low Energy (BLE)	26%
LoRaWAN	25%
NB IoT	23%
Sigfox	17%
Zigbee	16%

Emerging trends (continued)

DATA

While the majority of organisations are now gathering IoT data, there is still plenty more to do to derive maximum benefit from it. The ultimate measure of an IoT project's success is how it improves the way a company or its partner eco-system operates. This is largely resultant on the type of data extracted, and how it is shared and turned into insight.

Currently 80 per cent of respondents' businesses only share data within the organisation. However, in the future this is set to change with a larger proportion shifting toward sharing data with their wider supply chain. In theory this more co-operative method will be beneficial to all parties, but of course this will result in data privacy, security and sovereignty challenges that should be considered as part of an effective IoT strategy.

Security is predictably the foremost concern as a barrier for sharing data effectively, followed by a lag in data collection and availability, while in third place over a third of respondents admitted their lack of IoT data strategy was hampering their efforts. In relation to the second point respondents are clearly prioritising real-time (within a 30 second) data transfer, with the faster transfer the better. Only a very small proportion (4 per cent) are receiving their data points daily at the other end of the spectrum.

Why are you unable to use the data collected from IoT projects effectively?

54% Security/privacy concerns

46% Lag between data collection & availability

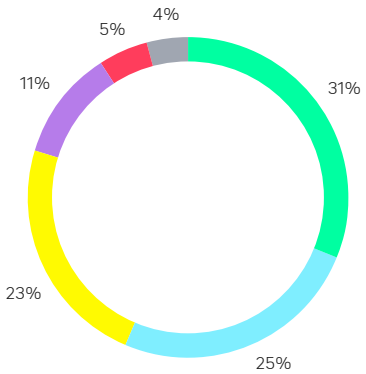
33% Lack of IoT data strategy

30% We lack skills to extract/use data

29% Data is stored in an unusable format

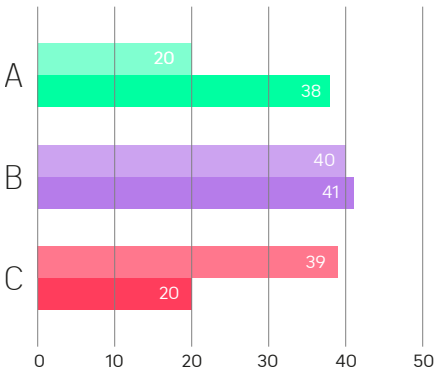
27% Data volume is too large

14% We are able to use data as effectively as possible



At what intervals do you gather data points in IoT projects?

- In real time
- Within half an hour
- Hourly
- Every two hours
- Every four hours
- Daily



To what extend does your organisation currently share non-sensitive data created through IoT projects?

A It is available to anyone in the organisation, or our partners, to access and use:
Currently In the future

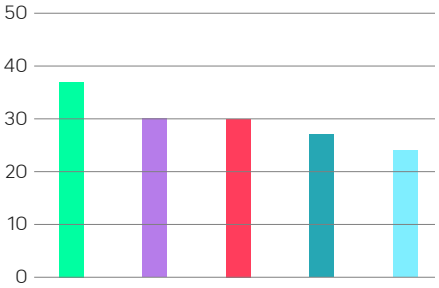
B It is available to anyone in our organisation to access and use:
Currently In the future

C It is only available to certain departments involved in the IoT project:
Currently In the future

SKILLS

Despite strong levels of IoT adoption across the board, the skills gap remains a concern. A lack of in-house skills remains the top barrier to IoT deployment, higher than other issues such as a lack of turnkey/off-the-shelf solutions, cost challenges and cyber-security risks. In terms of required skillsets, cyber-security talent is number one, closely followed by a need for additional staff with experience and skills in data science and analytics, technical support and connectivity technologies.

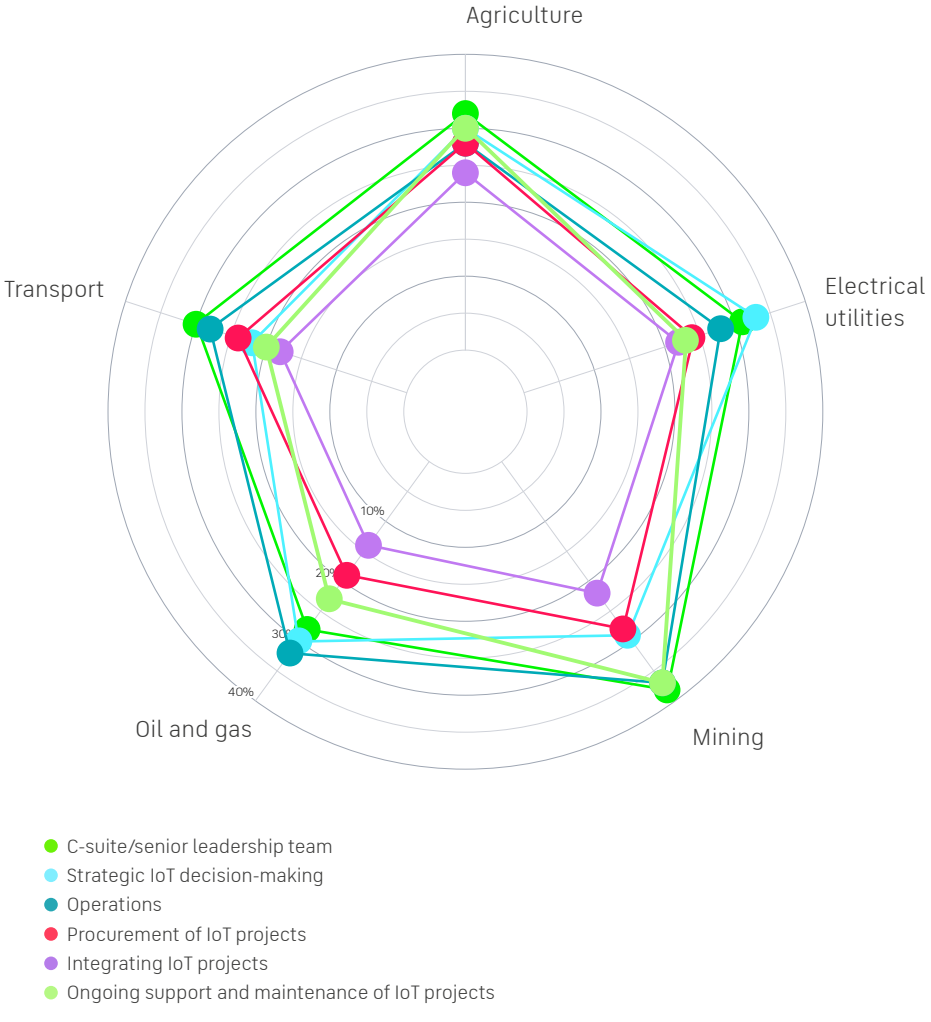
Additionally, a significant number of respondents still have a need for skills to drive the strategic development, management and procurement of IoT. Without all of these skillsets in place, businesses will continue to struggle to make the best use of the data they gather, to integrate IoT projects into the wider organisation and benefit from the transformative role that IoT can play in the global supply chain. If organisations do not have the resources to plug these gaps internally, they must look to external partners to provide the necessary skills.



What barriers to adoption does your organisation face in the deployment of IoT projects?

A lack of in-house skills	37%
Lack of turnkey/off-the-shelf solutions	30%
Security implications	30%
Lack of available capital to invest	27%
Lack of reliable connectivity	24%

Does your organisation have all the skills it needs to select, deploy and utilise IoT projects at the levels below?



What additional specific skills does your business need to deliver its IoT projects?

50% Security skills

49% Analytical/ data science skills

48% Technical support skills

47% Connectivity technology skills

42% Project management skills

39% Strategic skills

33% Procurement skills

27% Database management skills

Emerging trends (continued)

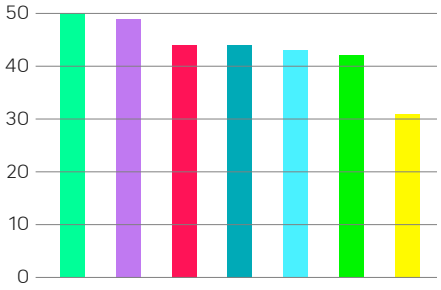
SECURITY

Whilst most organisations continue to face security challenges in the deployment of IoT solutions, the gravity of cyber-security issues are increasingly better understood, with measures being taken to remedy vulnerabilities. Nearly half (48 per cent) have responded to IoT security issues by creating an internal IoT security policy. Not only that, a greater proportion of organisations now also have an external IoT policy for suppliers and partners than was the case in 2018, which lays the groundwork for more businesses being able to share their data with third parties.

However, despite significant progress in addressing IoT security concerns most businesses still need to take more action to bolster their defences. Transport and logistics and mining businesses are the most confident in their approach to dealing with IoT security, while oil and gas organisations are least likely to state they have robust cyber-security measures from end-to-end. Given the risk that oil and gas organisations face from bad actors this is surprising, though it may reflect a heightened sense of awareness about the risks they face. This is supported by a much higher proportion of oil and gas respondents (59 per cent) than the overall set, answering that their cyber-security is good but could be improved.

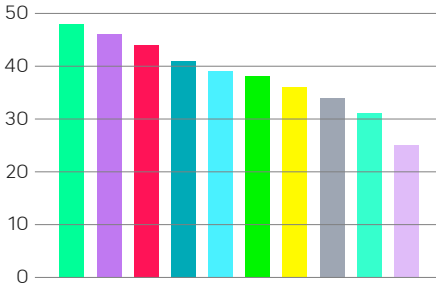
In terms of the types of threats posed, the risk of external cyber-attacks causes most concern, followed by poor network security, insecure/ unencrypted edge networks and employees mishandling data. In addition to investing in new security technologies, organisations must continue to train their employees on IoT security best practices.

"In terms of the types of threats posed, the risk of external cyber-attacks causes most concern."



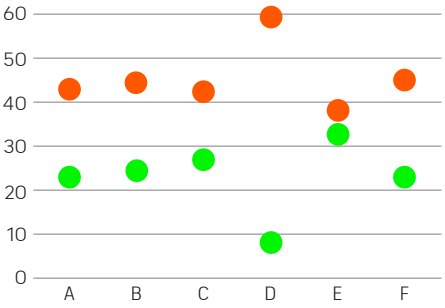
What are the biggest security challenges associated with the use of IoT projects within your organisation?

- Risk of external cyber-attack 50%
- Poor network security 49%
- Insecure/unencrypted edge networks 44%
- Potential mishandling/misuse of data by employees 44%
- Insecure storage of data collected 43%
- Internal data regulation and compliance requirements 42%
- Supplier/partner data regulation compliance requirements 31%



What changes to security is your organisation making to address IoT security concerns?

- Creation of an internal IoT security policy 48%
- Investing in new security technologies 46%
- Training employees on IoT 44%
- Creation of an external IoT security policy for suppliers and partners 41%
- Upgrading existing security technologies 39%
- Communicating to customers on the use of IoT 38%
- Partnering with a third party 36%
- Hiring skilled staff 34%
- Securing physical assets such as sensor nodes 31%
- Implementing a backup connectivity network 25%

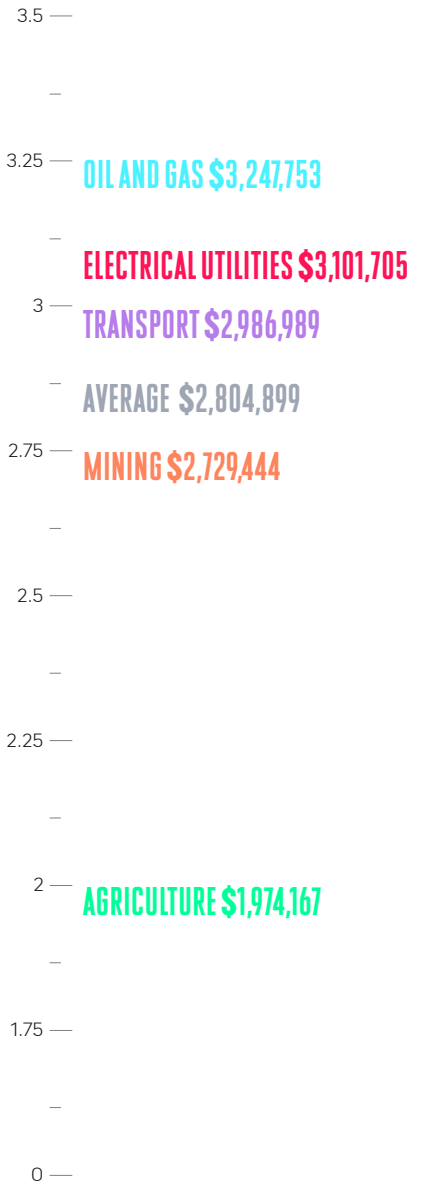


Which of the following statements best fits your organisation regarding the security of its IoT projects?

- My organisation's IoT solutions have robust cyber-security defences from end-to-end in compliance with the relevant ISO standard
- My organisation's IoT solutions have good cyber-security, but would still benefit from being stronger

A Agriculture
B Electrical utilities
C Mining
D Oil and gas
E Transport
F Average

What is your planned investment in IoT projects in the next three years?



What proportion of your organisation's IT budget do you expect to spend on the following digital transformation technologies over the next three years?

9.9% IoT projects

9.0% Cloud computing

7.5% Next generation security

7.3% Big data analytics

5.3% Robotics

4.8% Machine Learning

4.3% Virtual Reality

INVESTMENT

It is clear that IoT has reached a high level of maturity across most organisations, with businesses planning to invest the greatest proportion of their IT budgets on IoT projects over the next three years. Other digital technologies vying for IT budget include cloud computing, big data analytics, next gen security, robotics and machine learning technologies, with cloud computing being usurped from its position as the most invested in technology during the last three years. There are however noticeable variations in the planned levels of IoT investment, with oil and gas and electrical utilities planning on investing more than transport and logistics, mining and particularly agricultural companies.

This mainstream adoption of IoT is already making a significant difference in terms of operational cost-savings to many organisations, with a 15 per cent reduction in costs expected at the end of the next twelve months, rising to 30 per cent by 2026. Most optimistic at almost every date are mining respondents who expect IoT to deliver approximately 33 per cent in cost savings in five years' time.

What proportion of your organisation's costs are saved/going to be saved from its use of IoT projects?

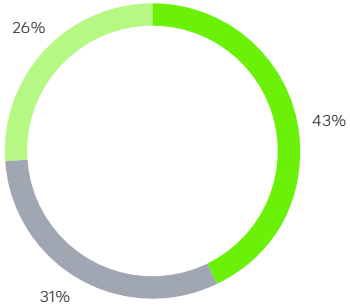
9% Currently

15% In 12 months

22% In 3 years

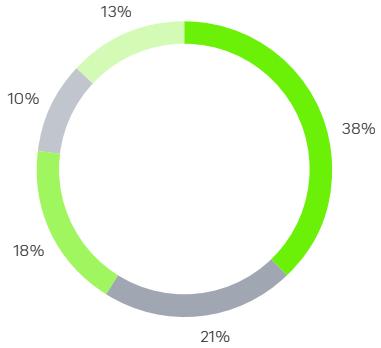
30% In 5 years

AGRICULTURE



Respondents by sub-sector (%)

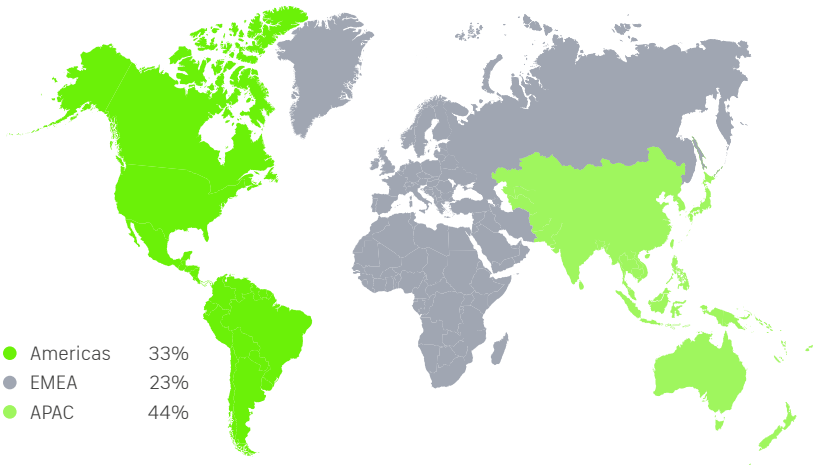
- Crop production
- Livestock
- Service providers



Respondents by size of organisation (%)

- 251-500 employees
- 501–1,000 employees
- 1,001–3,000 employees
- 3,001–5,000 employees
- More than 5,000 employees

Respondents by region (%)



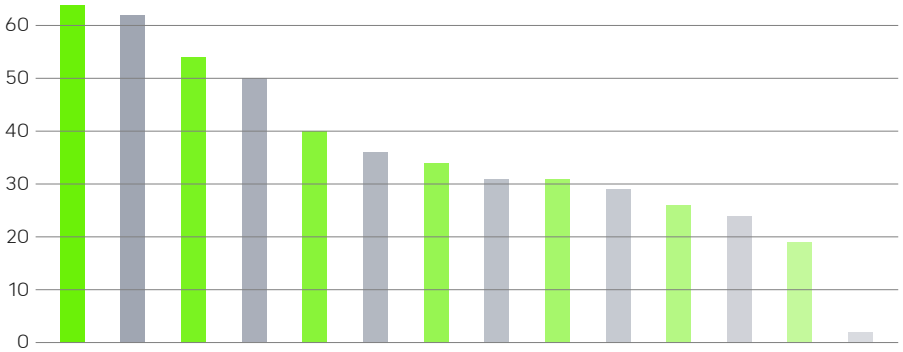
- Americas 33%
- EMEA 23%
- APAC 44%

According to the UN, the world will need to double its food production by 2050 in order to feed its growing population.[1] This means agricultural producers will need to increase production efficiency with the finite land available. Concurrently access to water poses a huge challenge, with a demand deficit predicted in the next ten years. Agricultural producers are also facing the long-term effects of increased extreme weather events due to climate change, as well as declining soil health and biodiversity loss.

Encouragingly there are clear signs that producers are taking these challenges seriously, adopting new technologies (AgTech) that can help them increase their outputs in line with demand. While agriculture also produces building materials, medicines and cosmetics, it is the area of food production where we can see the clearest example of technology being adopted to modernise production. Investment in technologies to bolster food production has increased by six times since 2012, up to $20 billion in 2019.[2] Technologies like genetic crop enhancement, precision agriculture and computational biology are germinating answers to one of humanity's greatest challenges: how to feed a growing population while limiting adverse effects on the environment.

The Internet of Things (IoT) is playing a key role for agricultural businesses across the entire production cycle. From helping growers understand water and nitrates in the soil, to providing cattle farmers with information regarding the health of their animals, to helping aquaculturists monitor the oxygen levels

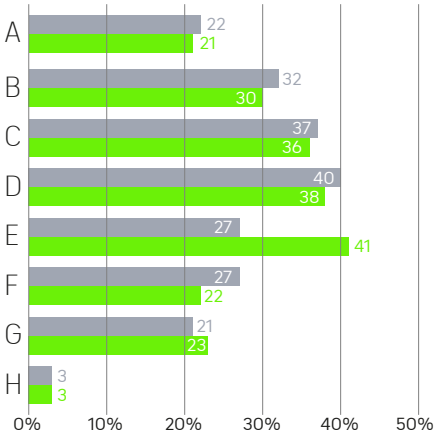
"Agricultural producers will need to increase production and distribution efficiency and do more with the land available to them."



What are the most important drivers for the deployment of IoT projects for your organisation?

Greater automation	64%	Improve compliance/regulatory	31%
Cost efficiencies	62%	Reduced downtime	29%
Greater supply chain insight	54%	Lower insurance premiums	26%
Improve environmental sustainability	50%	Improve customer experience	24%
Better decision-making	40%	New revenue streams	19%
Improve health and safety	36%	Other	2%
Increase staff productivity	34%	Don't know	0%
Greater physical security	31%		

"40 percent of agriculture respondents have a formal IoT strategy."



What barriers, if any, does your organisation face in the deployment of IoT projects?

- A Lack of consistent and reliable connectivity
- B Lack of available capital to invest in IoT projects
- C A lack of in-house skills
- D Lack of turnkey/off-the-shelf solutions
- E IoT not being prioritised by the board
- F Security implications
- G Integrating IoT technology with existing platforms
- H Not encountered any barriers at this stage
- Encountered in the deployment phase
- Encountered/expect to encounter this once deployed

[1] https://www.un.org/press/en/2009/gaef3242.doc.htm
[2] https://agfunder.com/

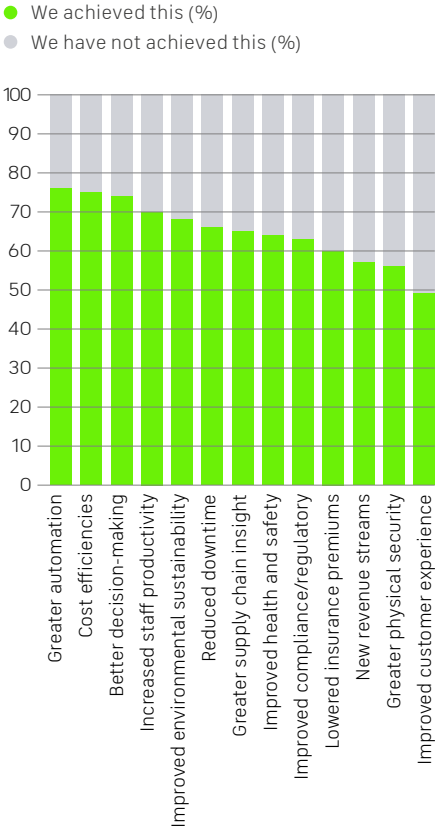
in their salmon pens, it is providing visibility and automation across production and supply chains, enabling businesses to operate in an informed manner, remotely. Key to organisations unlocking the potential of IoT is a formal IoT strategy, which 40 per cent of our agricultural respondents stated they have, although there is some difference between service providers (50 per cent), crop producers (41 per cent), and livestock producers (26 per cent).

The role of IoT has become all the more important during the Covid-19 pandemic where producers and supply chains have faced unprecedented challenges related to access, logistics and levels of changing demand. Our research suggests the operational impact of the pandemic has been more keenly felt by crop producers, than livestock producers or service providers. Additionally, 87 per cent of crop producers, 86 per cent of service providers and 83 per cent of livestock respondents have either accelerated deployment of IoT projects as a result of the pandemic or plan to in the next few years. It can be surmised that this will support automated operations in the face of local and national lockdowns.

Overall our research finds IoT in the sector at an inflection point: larger organisations of over 3,000 employees are clearly more progressed and are taking advantage of enterprise-level IoT solutions to optimise their more complex supply chains. Below this in the 250 – 3,000 employee bracket, organisations are starting to deploy IoT in greater numbers, driven by technologies that are becoming available at affordable price points and are focused on addressing burning problems with attractive value propositions. For example, availability of new, lower cost IoT sensors such as weather stations and soil moisture probes. With these two vectors aligned, the decision to deploy IoT becomes a no brainer even where budgets are a challenge, because agricultural businesses are seeing clear benefits to adoption, often within a single production cycle or season. These benefits are predicted to ramp up in line with adoption levels in the years to come so agricultural businesses will need to keep an eye on the challenges holding them back.

Budgets are a challenge for the sector, particularly for smaller companies, with these representing some of the lowest budgets of any group within our research. There are also a range of other business challenges that are stopping the sector from getting the optimal benefits from the technology. A shortage in skills is a critical issue that needs to be solved, while the sector still has a lot of progress to make in terms of building the connectivity backbone needed to make IoT a true success. Linked to this is the need to have effective and efficient data management tools and strategies in place, as well as the security capabilities to ensure the growing threat of cyber-attacks is kept at bay. To achieve these goals, the sector needs to be prepared to invest in the right areas, both now and in the immediate future.

How would you score your organisation's achievement of expected benefits of IoT projects?



ADOPTION

Over three-quarters of organisations in the agriculture sector (80 per cent) have fully deployed at least one IoT project, up from 22 per cent in 2018. 53 per cent have deployed fully within the last 12 months showing rapid levels of adoption in 2020, which points to IoT adoption in the sector beginning to reach maturity. The remaining 20 per cent of respondents either plan to deploy IoT within the next two years or are currently trialling such projects.

As with most industries, agriculture has been challenged by Covid-19, and caused many to rethink their approaches to technology as a way to gain an operational edge. 60 per cent say that challenges related to the pandemic have demonstrated the importance of IoT and automation to the success of their business. As a result of experiences in the pandemic, 86 per cent of our respondents have either sped up deployment of IoT projects, or plan to do so in the next couple of years. This represents agricultural producers fortifying their ability to operate remotely and autonomously and demonstrates the faith our respondents have in the technology.

The drivers that are motivating the sector to deploy IoT projects are numerous with greater automation cited as the most popular reason by 64 per cent of respondents. Not far behind is cost efficiencies (62 per cent), followed by; improved greater supply chain insight (54 per cent), improved environmental sustainability (50 per cent) and better decision making (40 per cent). Environmental sustainability was viewed as the most important driver of IoT usage in North America (92 per cent), while in APAC it was greater supply chain insight and everywhere else it was greater automation. Interestingly, in North America respondents listed the highest number of different drivers for using IoT suggesting a sophisticated understanding of IoT's potential.

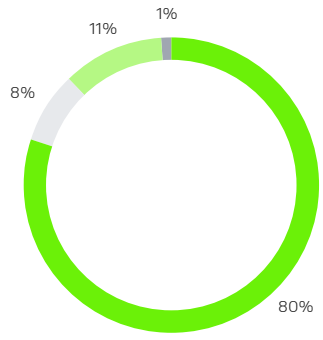
In terms of use cases the most common area IoT is being engaged is in remote water monitoring and control, where 27 per cent of respondents have already deployed IoT solutions, and an additional 22 per cent are in the trial phase. Crop storage monitoring was in second place with 26 per cent of respondents having actively deployed it.

In the next couple of years there is likely to be an increase in fully deployed IoT projects focused on weather and soil monitoring and process automation, with these two representing the most likely to be in trial currently (37 per cent and 33 per cent respectively). Of course this will be dependant on projects successfully moving through the trial phase, which isn't always the case. The most likely use cases to fail in the trial stage leading to them not being deployed was machinery and vehicle monitoring, as well as irrigation monitoring and control, both with 12 per cent. Some of the challenges contributing to these failed trials we will explore over the coming pages.

Beyond the farm, the sector is also recognising the need to gain better visibility of the supply chain. 24 per cent of respondents have already deployed IoT projects to improve supply chain traceability, while 29 per cent are in the trial phase. The larger organisations (over 3,000 employees) are ahead of the curve in this particular area, with 43 per cent having already leveraged IoT for supply chain management and an additional 33 per cent trialling it. These businesses are more likely to be supplying multi-nationals whose business models are dependent on complex digitalised supply chains.

Despite all of the progress barriers remain. During the deployment phase 40 per cent were challenged by a lack of skills, with 37 per cent feeling a lack of turnkey solutions hampered them and 32 per cent a lack of capital. The number of respondents indicating there was not enough capital available to optimally deploy was high compared with the other sectors we interviewed, reflecting the tighter budgets agricultural businesses are often faced with. Once projects were deployed respondents indicated the biggest barrier was the lack of IoT support at board level (41 per cent) suggesting the need for greater C-suite education regarding the benefits achieved.

By and large, the majority of respondents have achieved the expected benefits of IoT projects across a range of areas, including increased automation, cost efficiencies and better decision making. This is encouraging given these represented some of the most important drivers. However, there remain areas where these benefits have not yet been achieved. For example, 51 per cent say their IoT projects have not yet led to an improved customer experience, while 44 per cent say they have not attained enhanced physical security, although these were not such strongly desired outcomes across the agricultural respondents.



What is your current status in terms of deploying IoT projects?

- Fully deployed
- Currently trialling
- Planning to trial within 12 months
- Planning to trial in 18 months – 2 years

What IoT projects has your organisation already deployed and what will your organisation deploy in the future?

CONNECTIVITY

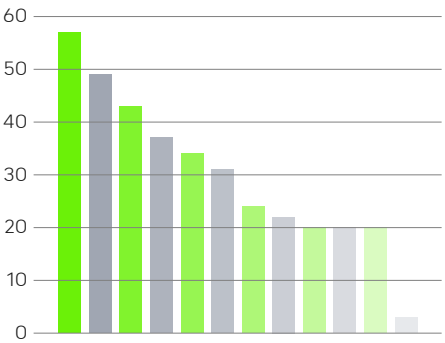
Connectivity, or the right kind of connectivity, is outlined as a key barrier to agricultural IoT adoption by McKinsey in recent analysis.[3] The good news is there are a range of connectivity technologies that can bring the benefits of IoT to the agriculture sector. These innovations help to overcome challenges related to the often remote situation of many farms and the associated lack of terrestrial connectivity infrastructure. These technologies are becoming available at a more accessible price-point and while our research focuses on large-scale agri-businesses, these technologies are also becoming more accessible to smaller businesses and increasingly to producers in developing economies.

Our respondents employ a wide range of connectivity types in their IoT projects, combining both short- and long-range technologies with three types used on average – common to our average across all sectors. Satellite figures most prominently in terms of long-range solutions (used by 49 per cent) while Wi-Fi is the most popular short-range connectivity type (57 per cent), despite its limitations in terms of range and power consumption. Since our 2018 report, adoption of Low Power Wide Area Networks (LPWAN) such as LoRaWAN have increased, likely because they are very suitable for connecting large numbers of devices over large areas.

Connectivity issues hampering the rollout of IoT projects are common. 59 per cent of respondents in the sector experienced difficulties deploying IoT because of connectivity issues in the areas they wanted to implement it, with 72 per cent encountering problems in the trial or proof of concept phase, and 64 per cent seeing issues after full deployment. There are, however, rewards to be reaped once these challenges are ironed out, as 78 per cent say that their IoT projects have been much more successful since mastering their connectivity woes.

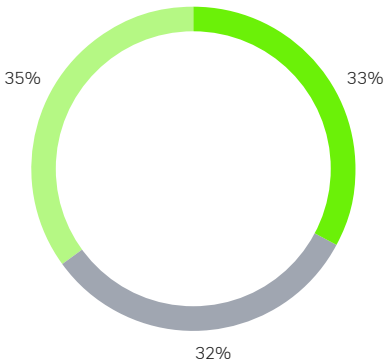
Respondents displayed a range of preferences in what qualities they wanted from their IoT connectivity. Reliability was most commonly cited, along with cost (both with 42 per cent), while network coverage, bandwidth and security followed (all with 34 per cent). Across the industries we spoke with reliability was the most desired attribute for IoT connectivity, however; the agricultural focus on cost concerns, where operational budgets are tighter than other industries are more unique to this sector. Budgetary challenges might also go some way to explain the usage of terrestrial connectivity types even if they are not completely suitable for the task.

While organisations are seeking the most reliable connectivity possible there are inevitably instances where there are outages. These become increasingly problematic when connectivity is underpinning the production process and downtime results in a loss of production; it is therefore essential that a backup connectivity method is considered. However; only 33 per cent of respondents utilise a backup connectivity option, while a further 67 per cent indicated their operations would go offline, with 32 per cent continuing to collect data offline and 34 per cent pausing all data collection until the connection is restored. Without reliable backup connectivity the development of use cases like autonomous vehicles or drones will be impossible, as the result of a connectivity failure could result in dangerous scenarios.



What connectivity types does your organisation use in its IoT projects?

Wi-Fi	57%
Satellite	49%
Radio	43%
Cellular (public)	37%
LoraWAN	34%
NB IoT	31%
Fibre	24%
Cellular (private)	22%
Bluetooth Low Energy (BLE)	20%
Sigfox	20%
Zigbee	20%
Other	3%



What do you do if unable to connect to your chosen connectivity type?

- Use a backup connection type to continue
- Continue collecting data offline until the connection is restored
- Pause all data collection until connection is restored

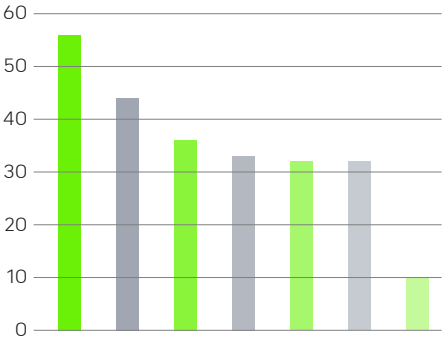
[3] https://www.mckinsey.com/industries/agriculture/our-insights/agricultures-connected-future-how-technology-can-yield-new-growth

DATA

The success of IoT projects can be measured in the actionable insights they create. To create optimal insights data needs to be with the right people, at the right time and in the right format. Like all of the sectors we surveyed, agricultural organisations still have some work to do in order to make full use of the IoT data they collect. The obstacles presenting effective data management are numerous, with security and privacy concerns the most prominent at 56 per cent. This is followed by a lag between data collection and availability at 44 per cent, echoing some of the connectivity challenges mentioned earlier. In third place the lack of an IoT data strategy was problematic for 36 per cent of respondents. More organisations should employ an IoT data strategy as part of their overall IoT strategy, as without this they are unlikely to get data to where it needs to go within the organisation let alone to other parts of the supply chain.

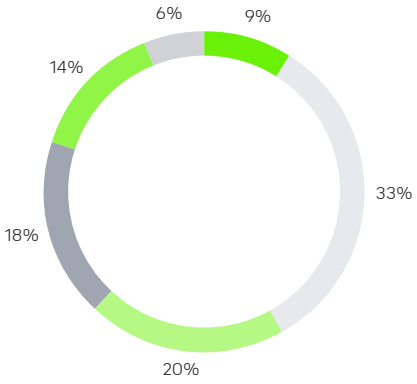
As far as data sharing is concerned, agricultural respondents are generally fairly open in approach, with 44 per cent making data available to anyone in the organisation, and an additional progressive 20 per cent sharing this with partners too. Just over a third, however, reserve access to this data to departments directly involved in IoT projects, which correlated with the group who did not possess a data strategy. In the future, agricultural organisations will increasingly share their data, to the point where just 18 per cent will limit data access to a select few departments. This is encouraging to see, as a culture of collaboration and joined-up thinking will help improve the efficiency of agricultural supply chains, though a data management strategy will be important to ensure the data only goes where it needs to.

In terms of the frequency that data is collected in agricultural projects, the sector has the lowest proportion gathering data in real-time (9 per cent), with only 4 per cent of the livestock respondents doing so. Businesses are most likely to collect data every half an hour (33 per cent), although hourly collection (20 per cent) and collection every two hours (18 per cent) are also common approaches. This is not that surprising as many IoT technologies today such as soil-moisture probes and weather stations require relatively infrequent data transfer. However, with greater automation being the largest driver for the deployment of IoT projects and new advances in technologies such as process automation and robotics coming on stream at a rapid rate the emphasis on real-time data is likely to increase.



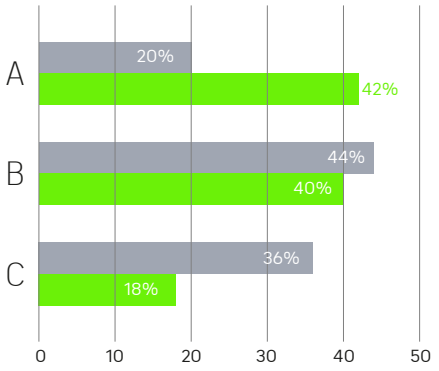
What barriers prevent your organisation from using data optimally?

Security/privacy concerns	56%
Lag between data collection and data being available	44%
Lack of IoT data strategy	36%
There is such a large volume of data we struggle to utilise it	33%
We don't have the skills to extract/use data	32%
Data is stored in an unusable format	32%
We are able to use data as effectively as possible	10%



At what intervals do you typically gather IoT data points?

- In real-time
- Within half an hour
- Hourly
- Every two hours
- Every four hours
- Daily



To what extent does/will your organisation share non-sensitive IoT data?

A It is available to anyone in the organisation, or our partners, to access and use

B It is available to anyone in our organisation to access and use

C It is only available to certain departments involved in the IoT project

Currently In the future

SKILLS

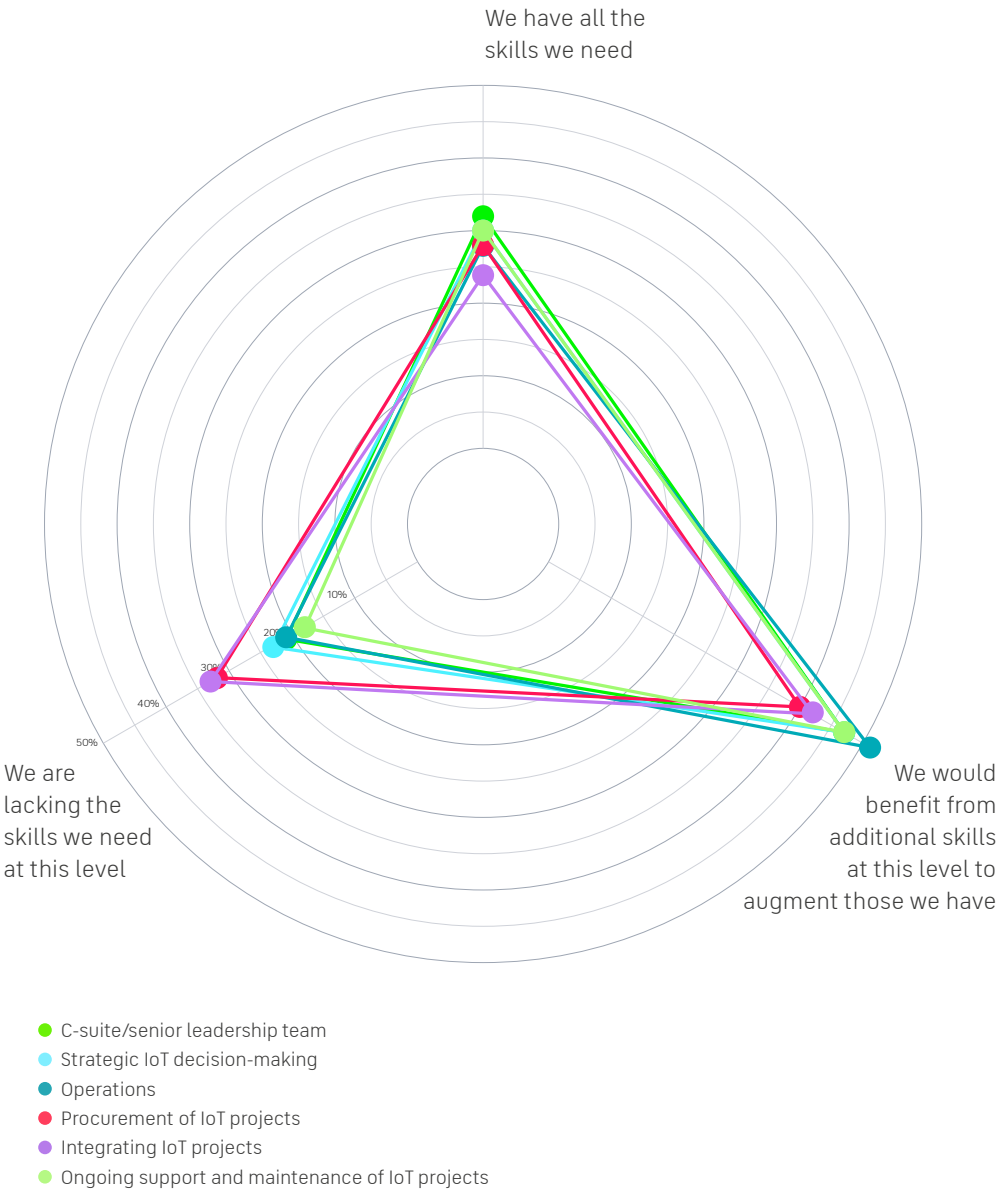
For IoT to be a sustained success access to the relevant skillsets is needed at all levels. Considering the number one barrier to successful IoT adoption is a lack of the right skillsets, this needs to be fixed urgently either through hiring, upskilling or working with a service provider.

Under a third of all respondents thought that they had all the skills required in-house to successfully deploy IoT projects, with many believing that they would benefit from additional skills to augment what they already have.

The most skilled personnel were found at C-suite level (32 per cent), whilst the least number of sufficiently skilled workers were found at the integration level (24%). This is perhaps not surprising given the challenges around data and hardware interoperability that are experienced in the agriculture sector, with numerous technologies available, not all of which integrate with one another.

"The number one barrier to successful IoT adoption is a lack of the right skillsets."

Does your organisation have the skills needed to fulfil IoT projects at different levels?

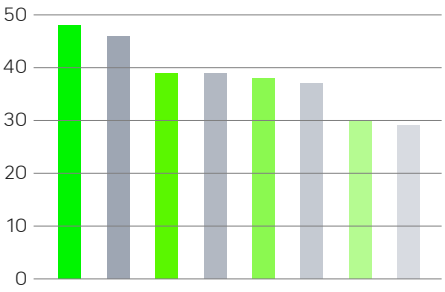


Service providers tended to possess more IoT related skills, and this is not surprising since they are often developing the technology and can sometimes be responsible for installing and managing it on farm. Latin American respondents were more likely to indicate they were lacking skills at all levels, while smaller organizations were more likely to be lacking the procurement skills to ensure they brought on onboard the right IoT solutions.

To address deficiencies, analytical and data science skills are most sought after (cited by 48 per cent), followed by connectivity technology skills (46 per cent) and technical support skills (43 per cent). Many businesses are focused on improving their data analytics capacity as it represents a critical step in taking data and turning it into actionable insight. Organisations of over 3,000 employees were much more likely to seek skills in this area, no doubt driven by deployed projects producing large quantities of data that needs to be turned into business enhancing insights.

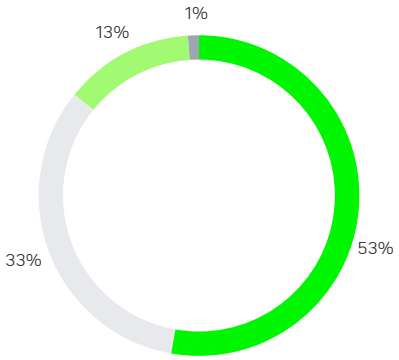
When it comes to purchasing decisions for IoT projects, the most common decision maker is middle management. However; smaller businesses are much more likely to have C-suite and senior management involvement, while for the largest businesses it is typically a middle management decision. To some extent this difference in methodology reflects the number of employees at an organisation, although it is important that larger organisations still incorporate an IoT focus at board level, even if decision making for specific projects is delegated.

Roughly half of those polled (53 per cent) are aware of off-the-shelf IoT solutions that can help them meet their organisation's needs, with this figure rising with the size of the organisation (41 per cent for companies under 3,000 employees versus 78 per cent for those with more than 3,000). This underlines the maturity and spending power of larger organisations as well as established strategic partners serving their part of the market. At the other end of the spectrum, service providers focused on smaller scale companies clearly have some work to do to create propositions addressing the challenges of smaller producers where the value proposition for the major drivers such as automation is less compelling.



What additional skills do you need to deliver IoT projects?

Analytical/ data science skills	48%
Connectivity technology skills	46%
Project management skills	39%
Technical support skills	39%
Strategic skills	38%
Security skills	37%
Database management skills	30%
Procurement skills	29%



Are you aware of off-the-shelf IoT solutions that meet your needs?

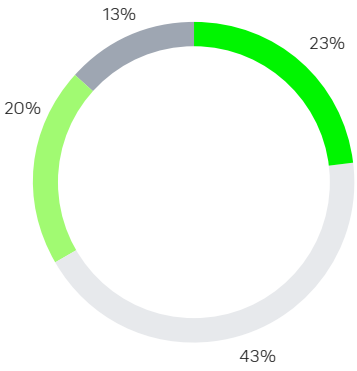
- Yes, we are aware
- No, providers only meet some of our needs
- No, providers don't meet our needs at all
- Don't know

SECURITY

While agricultural businesses may not immediately seem like a target for bad actors, the risk is increasing as businesses are putting more onus on their digital operations as a way of boosting their output. Anything which hampers production or leads to delays in supply could have dire repercussions for a company, its valuation and place in a supply chain, or if carried out on large enough scale, for consumers. It is not just cyber-attacks agriculturalists need to be wary of either. Misused or misplaced data could easily give competitors a huge advantage, stressing the importance of effective IoT security and data management strategies.

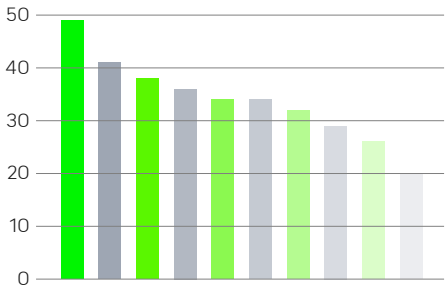
Agricultural respondents listed poor network security as the clear leader in terms of their security challenges, with half of those surveyed stating it as an issue. Businesses will need to harden their networks to avoid these perceived risks being exploited. Internal data regulation (46 per cent) is also seen as a key challenge to overcome, as is the misuse of data by employees (42 per cent), while the risk of cyber-attack was stated as a risk by 41 per cent. These worries are reflected in respondents' opinions of the security of their IoT projects. A total of 76 per cent believe that IoT security needs to be strengthened in some way, with 33 per cent of these wanting to see major improvements. Encouragingly, a relatively small amount of respondents have not prioritised cyber-security threats at all with all of these responses found in businesses under 3,000 employees and predominantly between 251-500 personnel.

In response to the perceived threats it faces the sector is carrying out a range of activities to tackle security problems, with external IoT security policies (49 per cent), partnering with a third party (41 per cent) and specific IoT training for staff the most common (38 per cent). Larger organisations are more likely to be addressing security issues in-house while smaller organisations are more reliant on third-parties to help sure up their defences.



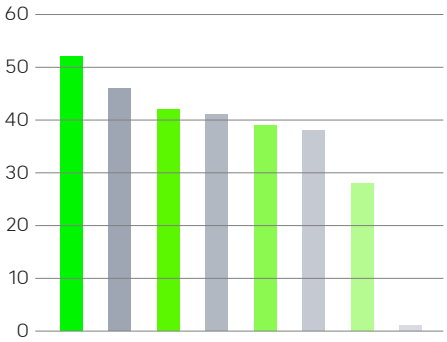
Which of the following statements are accurate regarding the security of your IoT projects?

- We have robust cyber-defences
- Our defences are good but could be stronger
- We need much better cyber-defences
- Our cyber-defences need to be vastly improved



What changes have you made to address IoT security concerns?

Creation of an external IoT security policy for suppliers and partners	49%
Partnering with a third party	41%
Training employees on IoT	38%
Investing in new security technologies	36%
Securing physical assets such as sensor nodes	34%
Creation of an internal IoT security policy	34%
Upgrading existing security technologies	32%
Communicating to customers on the use of IoT	29%
Hiring skilled staff	26%
Implementing a backup connectivity network	20%



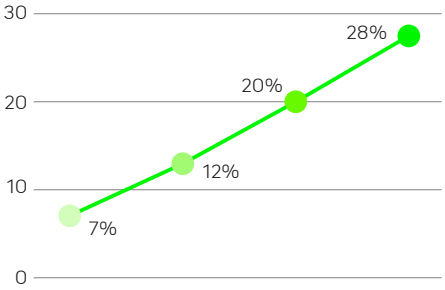
What are your biggest IoT security challenges?

Poor network security	52%
Internal data regulation and compliance requirements	46%
Potential mishandling/misuse of data by employees	42%
Risk of external cyber-attack	41%
Insecure/unencrypted edge networks	39%
Supplier/partner data regulation compliance requirements	38%
Insecure storage of data collected	28%
We have/ will not face any security challenges	1%

INVESTMENT

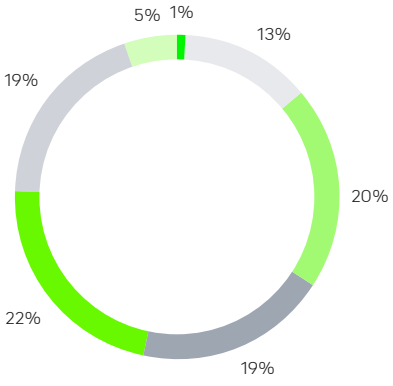
IoT budgets for the agriculture sector were significantly smaller than the other sectors we surveyed. On average the planned spend on IoT projects in the next three years is $1,974,167, with service providers understandably spending more ($2,178,571), followed by crop producers ($1,931,410) and livestock producers ($1,797,826). While this is similar to the other sectors we survey as a percentage it is considerably lower in real terms versus the average of $2,804,899. However, spend on IoT amongst agriculturalists grew depending on the size of the organisation, ranging from an average of $1,440,206 in companies below 500 employees to $4,796,250 for those with more than 5,000. Despite these differences in terms of size, it is clear to see that IoT ranks comfortably ahead of other digital technologies across the board.

Another encouraging sign is that respondents in the sector have a strong awareness of the potential for IoT to save the business money both in the short and long term. Currently, the average estimated saving for the business is 7 per cent, with this expected to rise to 12 per cent in 12 months, before eventually reaching 28 per cent in five years. This final figure is only slightly behind the wider sample average and given the fine margins in agriculture, points toward an optimistic future. Larger organisations with over 3,000 employees that can exploit greater yields and therefore gains, expect to see an even larger saving in the long term, expecting an average of 38 per cent in five years.



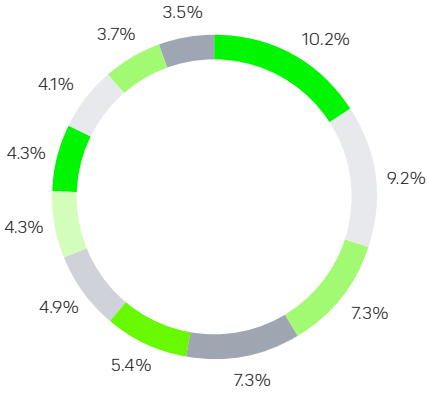
What proportion of your organisation's costs are saved/going to be saved from IoT projects?

Currently	7%
In 12 months	12%
In 3 years	20%
In 5 years	28%



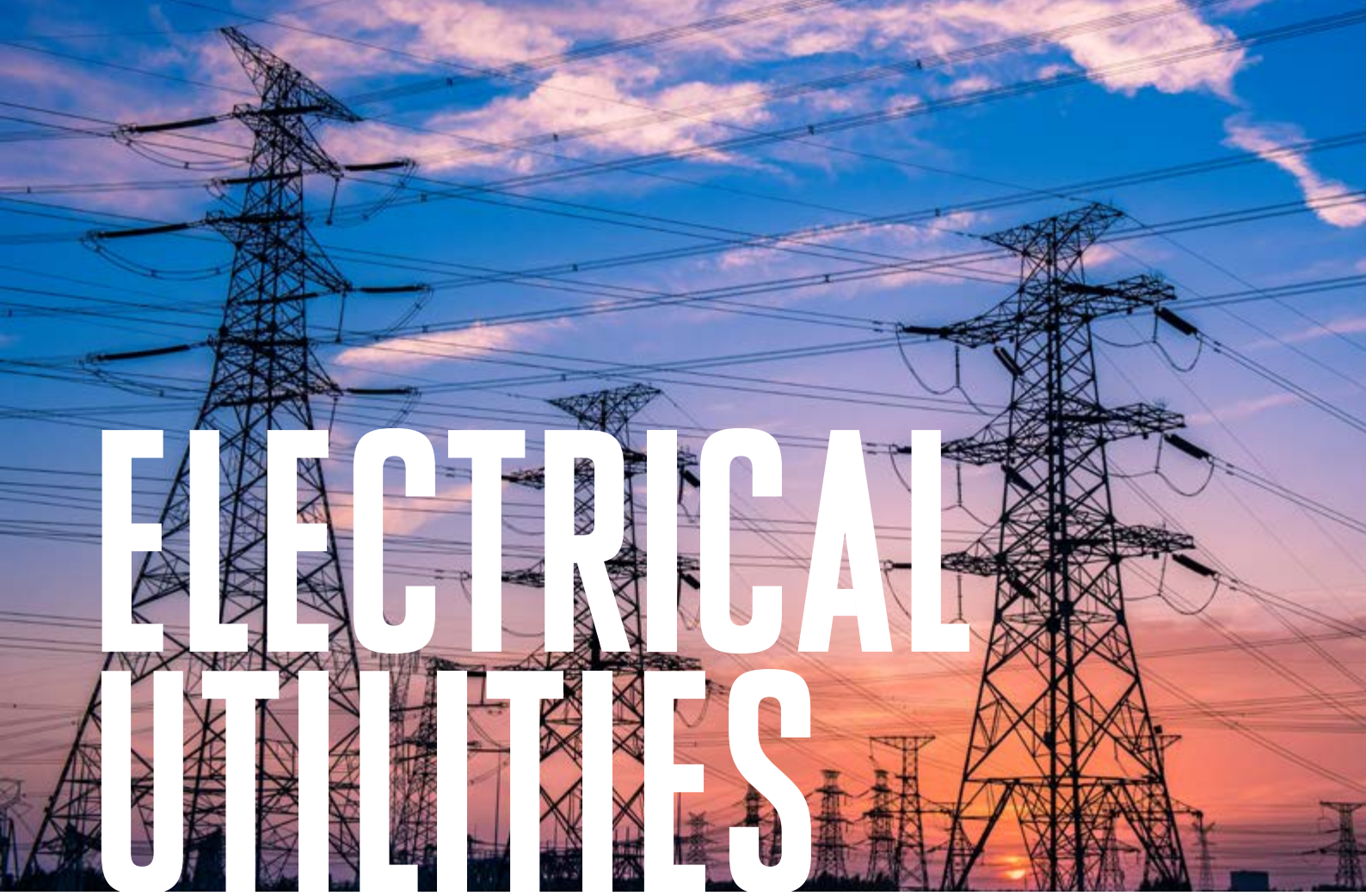
What is your planned investment in IoT projects in the next three years?

- $0 to $100,000
- $100,000 to $500,000
- $500,000 to $1,000,000
- $1,000,000 to $2,000,000
- $2,000,000 to $3,000,000
- $3,000,000 to $4,000,000
- $4,000,000 and above

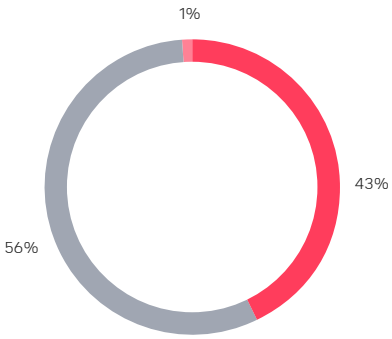


What proportion of your IT budget will you spend on IoT projects in the next three years?

- IoT projects
- Cloud computing
- Big data analytics
- Next generation security
- Robotics
- Augmented Reality
- Virtual Reality
- Machine Learning
- Cognitive AI
- Blockchain
- 3D Printing

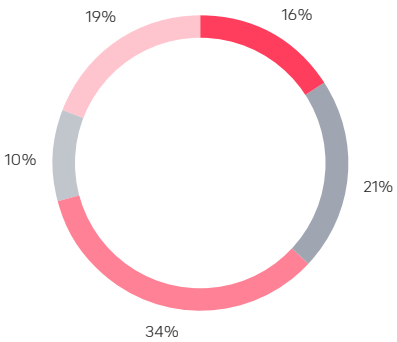


ELECTRICAL UTILITIES



Respondents by sub-sector (%)

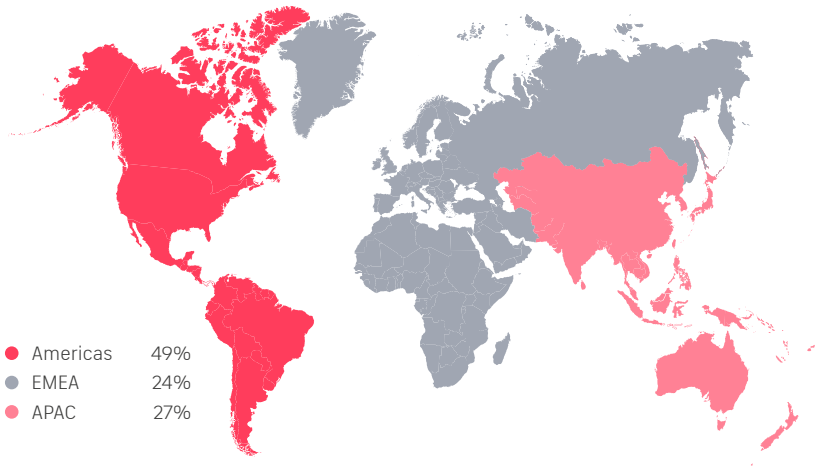
- Energy suppliers
- Energy distribution network operators
- Other



Respondents by size of organisation (%)

- 251-500 employees
- 501–1,000 employees
- 1,001–3,000 employees
- 3,001–5,000 employees
- More than 5,000 employees

Respondents by region (%)



- Americas 49%
- EMEA 24%
- APAC 27%

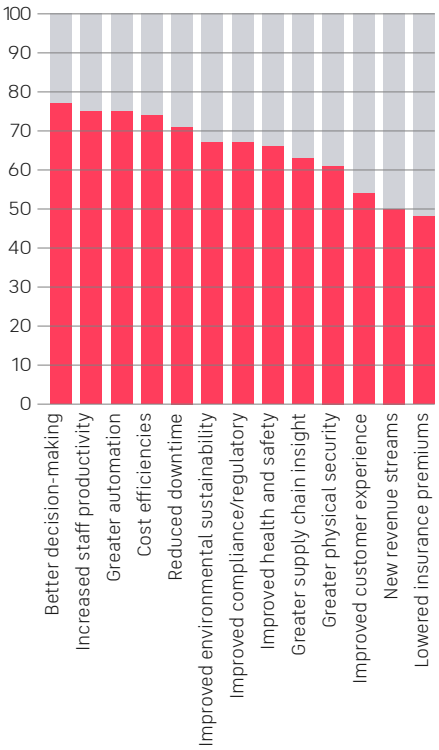
Humans have been consuming more energy year on year. Electric vehicles, growth in industry and an emergent global middle-class are some of the key factors behind this phenomena. By 2040 the International Energy Agency expects global energy to increase by 37 per cent.[1] In response, energy producers and distributors have been implementing digital technologies to boost their efficiencies and meet this demand.

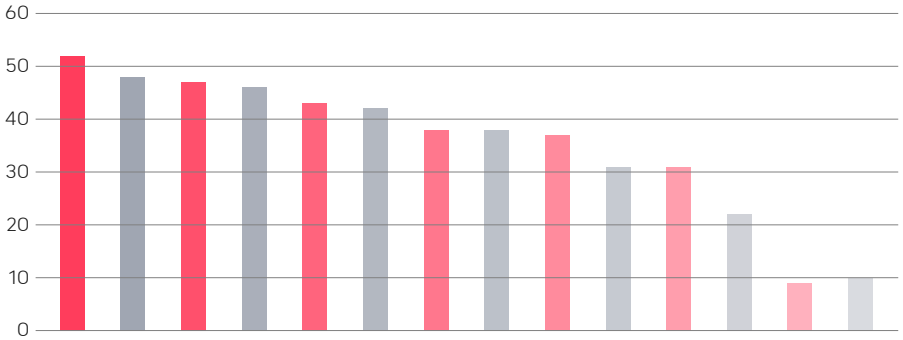
Lockdowns caused by the Covid-19 pandemic in 2020 caused electrical consumption in many parts of the world to drop 20 per cent from 2019 levels, before they came back to pre-Covid levels as societies opened up again.[2] While residential energy demand increased, it did not counterbalance the drop in use amongst commercial operations. While this period was unexpected and somewhat unprecedented, it has only underlined the importance of energy producers and distributors being able to effectively monitor and control their operations.

The ability to cope with these massive changes in demand was mitigated by work the industry has been undertaking over the last two decades. Many utilities companies have adopted digitalisation to develop new ways to monitor, manage, automate and improve the cost of production, their environmental footprint and the reliability of energy being supplied to businesses and consumers. The industry's approach has been to invest heavily in automation, command and control and communications technologies - the Internet of Things (IoT) - accelerating the evolution of ever 'smarter' electricity generation and distribution networks.

Unlike the traditional electrical grid, which was a 'one-way' system with power going from the grid operator to the customer, without any feedback and data going back to the provider, the modern 'smart' grid is a 'two-way' system. This is helping to overcome the financial costs of locating and fixing points of failure, outages and inefficient loadbalancing. The end result is more efficient operations, leading to better customer experience and compliance

How would you score your organisation's achievement of expected benefits of IoT projects?





What are the most important drivers for the deployment of IoT projects for your organisation?

Cost efficiencies	52%	Improve customer experience	38%
Better decision-making	48%	Reduced downtime	37%
Increase staff productivity	47%	Greater physical security	31%
Improve environmental sustainability	46%	Greater supply chain insight	31%
Improve health and safety	43%	New revenue streams	22%
Improve compliance/regulatory	42%	Lower insurance premiums	9%
Greater automation	38%	Other	10%

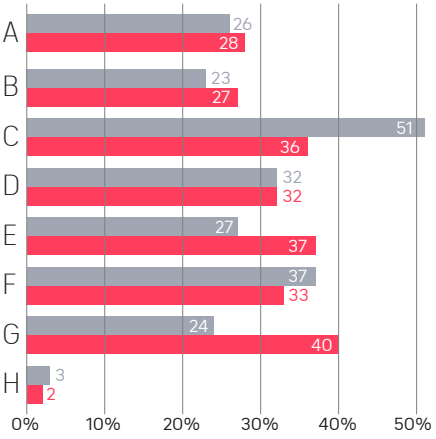
with government stipulated regulations around uptime and outages. Increasingly common IoT use cases such as distribution automation, using remote control resclosers, or advanced metering infrastructure (AMI) via smart meters provide utilities companies more opportunity to offer value back to consumers, through accurately tracking, forecasting and planning their energy consumption. Utility companies are expected to save $157 billion in costs from smart meters alone by 2035, according to recent forecasts.[3]

Reliable and secure connectivity is a vital enabler for supporting these technologies and organisations are using a blend of connectivity types to provide the ability to receive this data, often in real-time. While satellite was ranked as an important enabler its adoption remains lower than some terrestrial types, although this may be set to change given the dissatisfaction expressed by respondents for cellular and fibre to connect IoT projects. 58 per cent of businesses are still struggling to deploy IoT because of unreliable or inconsistent connectivity in the areas they wish to introduce it, and satellite could play a key role in supporting this process.

As with all industries, Covid-19 has also served to accelerate digital transformation and IoT adoption across the electrical utilities sector. Nearly half of respondents (48 per cent) claim that challenges related to the pandemic have underlined the importance of IoT and automation to business success. The same proportion (48 per cent) have accelerated IoT deployment in direct response to challenges associated with the pandemic, with an additional 36 per cent intending to start to accelerate their IoT projects over the next two years for the same reason. Overall, our research finds that the sector is reaching relative maturity in terms of IoT adoption levels, with 80 per cent of all organisations having fully deployed at least one IoT project. Larger organisations, as well as those in North America, Europe and APAC are the most advanced in terms of IoT adoption levels and planned IoT investments. However, despite the high level of maturity there are still a number of challenges ahead for the sector to ensure businesses get the optimal benefit from their IoT investments.

The sector is incredibly cyber-security conscious due to its position in a nation's critical infrastructure backbone and this theme factors into respondents' thinking at almost every stage of our survey. Security implications are cited more highly as a barrier to IoT deployment than in any other sector. Security is also the biggest concern prohibiting data sharing. Additionally the most desired skills are in cyber-security. The positive side of this cyber-security conscious outlook will see the sector respond in-step with emerging threats - the challenge may be to share data to drive value chain efficiencies.

"The International Energy Agency expects global energy demand to increase by 37 per cent by 2040."



What barriers, if any, does your organisation face in the deployment of IoT projects?

A Lack of consistent and reliable connectivity
B Lack of available capital to invest in IoT projects
C A lack of in-house skills
D Lack of turnkey/off-the-shelf solutions
E IoT not being prioritised by the board
F Security implications
G Integrating IoT technology with existing platforms
H Not encountered any barriers at this stage
● Encountered in the deployment phase
● Encountered/expect to encounter this once deployed

[1] https://www.iea.org/reports/world-energy-outlook-2020
[2] https://www.iea.org/reports/covid-19-impact-on-electricity
[3] https://www.smart-energy.com/industry-sectors/data_analytics/iot-for-utilities-harnessing-big-data-from-grids-edge

ADOPTION

The electrical utilities sector is reaching maturity in IoT adoption, with 80 per cent of organisations having fully deployed at least one IoT project to date. The last year has seen a notable acceleration in adoption, with 42 per cent of respondents having fully deployed over the last 12 months. The remaining 19 per cent of respondents are either currently trialling IoT projects, or plan to deploy them within the next two years.

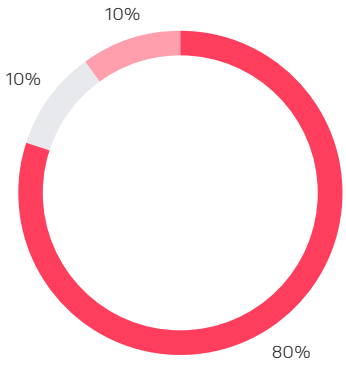
There are a number of key drivers motivating the sector to deploy IoT projects. Improving cost efficiencies is the most frequently stated reason, cited by 52 per cent of respondents. Not far behind is better decision making (48 per cent) and increased staff productivity (47 per cent), followed by improvements in environmental sustainability (46 per cent), health and safety (43 per cent) and compliance (42 per cent). There is some regional variation in these areas, with 71 per cent of respondents in North America citing improvements in environmental sustainability as a key driver for the deployment of IoT projects, compared to only 23 per cent in Europe. Plus, there are also differences between sub-sectors, with 54 per cent of energy generators citing greater automation as an important IoT driver, compared with only 26 per cent of network operators.

Greater automation, as well as achieving improvements in environmental sustainability and health and safety, are also higher priority IoT drivers for larger organisations. 78 per cent of respondents from organisations with 3,001 to 5,000 employees cite greater automation as a key IoT driver, while 71 per cent of businesses with over 5,000 employees cite improved health and safety.

In terms of use cases, the high level of maturity in the sector is reflected in the adoption rates of specific IoT projects. 56 per cent of energy network operators have either deployed or are currently trialling IoT in recloser monitoring and control, 40 per cent in substation monitoring and energy generation, and 38 per cent in vehicle tracking and people tracking to enhance health and safety. For energy suppliers substation monitoring (54 per cent), energy generation (51 per cent) and metering backhaul (46 per cent were the most common IoT projects adopted.

Despite high levels of adoption, there are still a number of key barriers to IoT deployment, largely related to issues with skills, security and a perceived lack of suitable IoT solutions. During the deployment phase of an IoT project, 51 per cent of respondents said that a lack of in-house skills was a problem, 37 per cent cited security implications and 32 per cent said a lack of turnkey or off-the-shelf IoT solutions was an issue. The number of respondents indicating that both skills and security were barriers to optimally deploying IoT are higher than any other sector we interviewed. Once projects were deployed, the two main barriers utilities companies encountered were integrating IoT technology with existing platforms (40 per cent) and IoT not being prioritised by the board (37 per cent).

Overall, the majority of respondents have either already achieved, or expect to soon achieve the benefits of IoT in terms of increased staff productivity, better decision-making, greater automation, improved environmental sustainability and greater supply chain insight. However, while these findings are encouraging, there is still plenty of work to be done by utilities businesses in the coming years to maximise IoT's potential. For example, 37 per cent say their IoT projects have not yet led to an improved customer experience, while 36 percent say they have not yet attained enhanced physical security.

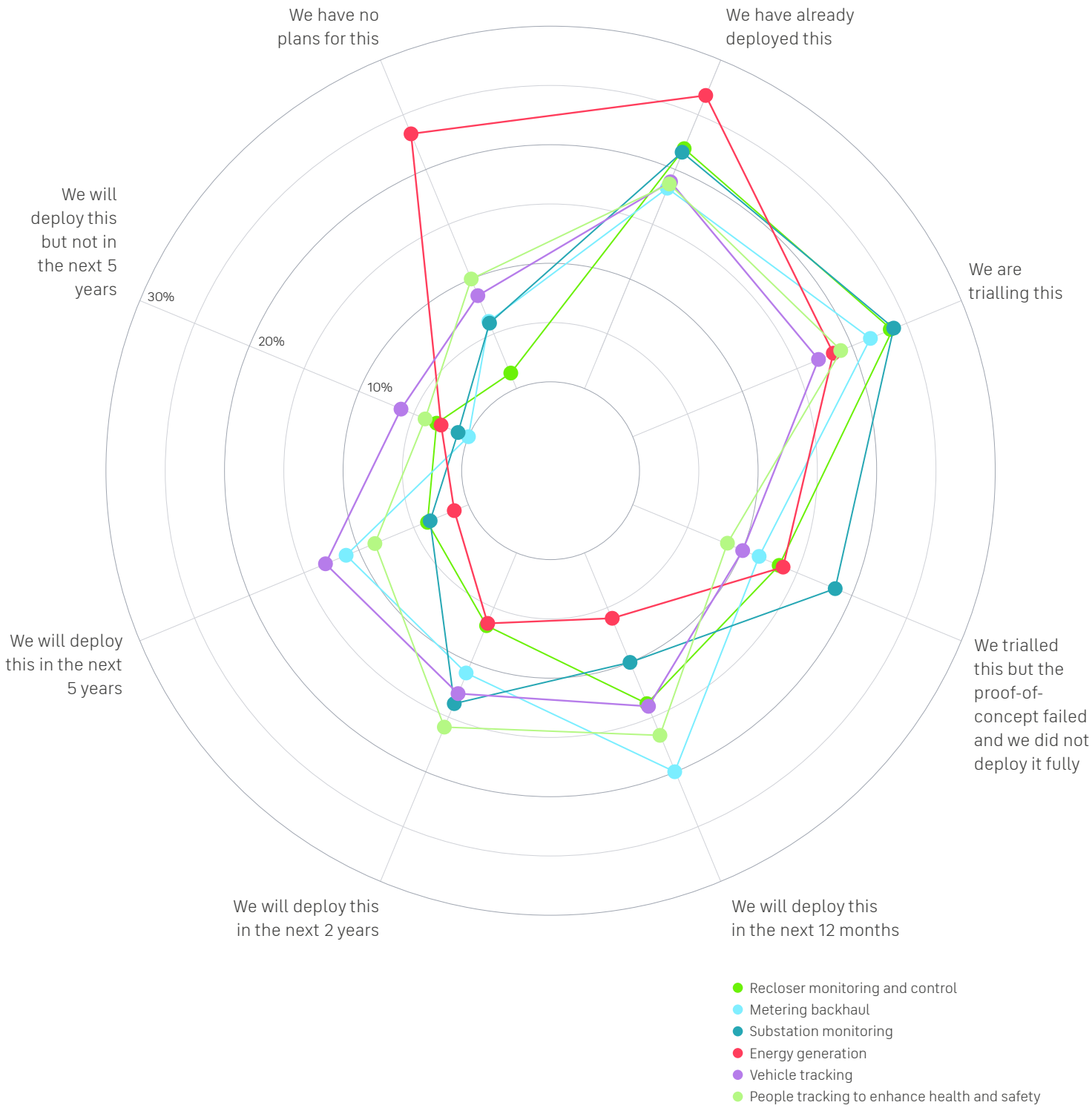


What is your current status in terms of deploying IoT projects?

- Fully deployed
- Currently trialling
- Planning to trial within 12 months

"48% of electrical utilities organisations have a formal IoT strategy."

What IoT projects has your organisation already deployed and what will your organisation deploy in the future?



CONNECTIVITY

Our results reveal that connectivity continues to be a key barrier to IoT adoption in the sector, as the industry continues to shift from the traditional unidirectional grid towards a smarter grid. The majority (59 per cent) of electricity suppliers and 36 per cent of energy network operators say that public terrestrial networks such as cellular or fibre are either not really or not at all suitable for their needs in order to deploy IoT projects. This figure increases to 85 per cent in Latin America, highlighting the particular need for reliable, non-terrestrial connectivity for businesses servicing highly remote and rural areas where terrestrial connectivity is either unreliable or non-existent.

While this view on terrestrial connectivity may be held by many respondents, the connectivity types being used in IoT projects do not necessarily follow this thinking. From a long range connectivity perspective, public cellular networks are the most popular choice (38 per cent), followed by radio (36 per cent), and fibre (34 per cent). These responses likely reflect a focus on static assets in relatively populous areas, as with a distribution grid for a city; however, it is evident that for IoT projects in remote areas, where these connectivity types may not be suitable, another approach is needed.

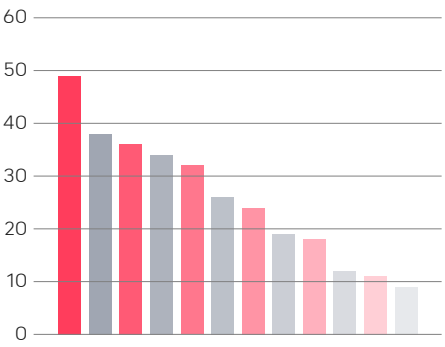
Our respondents stated that satellite is only in use in 32 per cent of organisations across the sector as a whole (rising to 38 per cent amongst electricity suppliers). The use of satellite in IoT projects is notably lower in the electrical utilities sector in comparison with all the other industry sectors we interviewed, where it averages 47 per cent across the board. This was an interesting finding and suggests satellite suppliers need to do more to work with electrical utilities companies to educate and build the right solutions. Regionally satellite usage was greater in APAC and Latin America than in North America where public cellular usage was proportionately higher.

In terms of shorter range connectivity types, both energy suppliers and energy distributors remain heavily dependent on Wi-Fi (44 per cent and 52 per cent, respectively), which is still by far the most popular short-range connectivity type. Following this Long Range Wide Area Networks (LoRaWAN) and Bluetooth Low Energy (BLE) are being used by 19 per cent and 18 per cent of respondents respectively.

Connectivity issues continue to obstruct the successful roll-out of IoT projects by electrical utilities organisations, with 58 per cent of businesses still struggling to deploy IoT because of unreliable or inconsistent connectivity in the areas they wish to introduce it. 75 per cent of organisations encountered connectivity problems in the trial or proof of concept phase of IoT, while 62 per cent continued to discover connectivity challenges causing disruption after full deployment. However, once connectivity challenges are solved, 80 per cent of organisations in the sector have enjoyed more success with IoT.

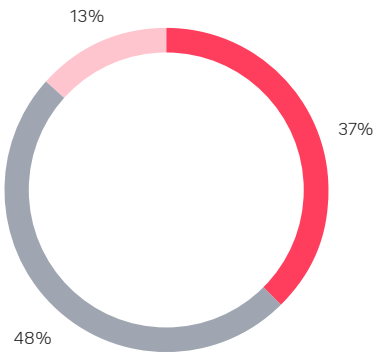
Respondents displayed a range of preferences in what qualities they wanted from their IoT connectivity. Security (56 per cent) and reliability (48 per cent) are the most commonly cited, followed by network coverage (36 per cent), bandwidth/speed (32 per cent) and cost (30 per cent). With the sector prioritising secure connectivity over any other attribute, and more so than any other sector, it is surprising that the use of public cellular networks and Wi-Fi is so high. Other connectivity forms, such as L-band satellite, could provide more reliable, more secure and less contended options.

Reliable connectivity is a priority for IoT, but organisations should ensure they have a backup plan in place to so that data can still be transferred in the event of a connectivity outage. In the event our respondents are not able to access their primary connectivity type, 37 per cent will switch to a backup connectivity type to continue the transfer of data - a figure significantly above other sectors. A further 61 per cent stated their operations would go offline, with 48 per cent continuing to collect data locally and 13 per cent pausing all data collection until the connection is restored. Pausing data collection was far less likely amongst North American, APAC and European respondents compared with their Latin American counterparts.



What connectivity types does your organisation use in its IoT projects?

Wi-Fi	49%
Cellular (public)	38%
Radio	36%
Fibre	34%
Satellite	32%
Cellular (private)	26%
NB IoT	24%
LoraWAN	19%
Bluetooth Low Energy (BLE)	18%
Zigbee	12%
Other	11%
Sigfox	9%



In remote areas away from terrestrial communication, what do you do if unable to connect to your chosen connectivity type?

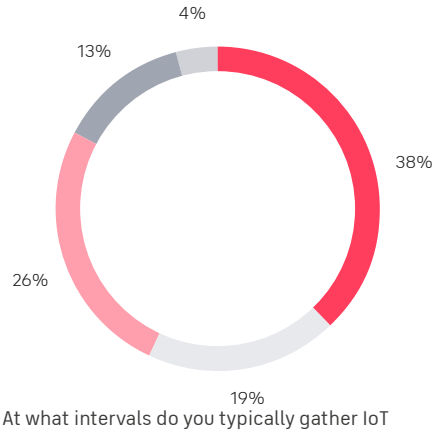
- Use a backup connection type to continue
- Continue collecting data offline until the connection is restored
- Pause all data collection until connection is restored

DATA

Electrical utilities organisations are leveraging the IoT to generate valuable data from all the points across the lifecycle between energy suppliers, distribution network operators and consumers. Our study reveals a number of reasons why utilities organisations are not able to use data from their IoT projects as effectively as possible. Chief amongst these are security and privacy concerns at 53 per cent and a lag between data collection and availability at 44 per cent, which reflects some of the connectivity challenges mentioned earlier. Following these fundamental data security and privacy issues, data being stored in an unusable format was problematic for 38 per cent of respondents and 33 per cent of organisations still lack a coherent IoT data strategy. Without a coherent IoT data strategy in place, utilities businesses will struggle to extract actionable business insights from the data they create.

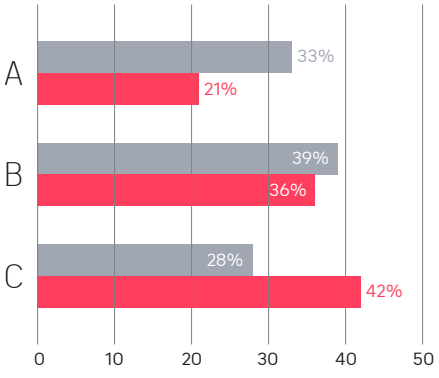
Sharing data in a timely way to all parts of the electrical utilities value chain is key for improving efficiencies and ultimately building customer satisfaction. Both within and between organisations in the sector, this is still an area that needs considerable improvement. With 42 per cent of respondents currently only making IoT data available to those departments directly involved in IoT projects and only 21 per cent making this data available to anyone in the organisation, or its partners, to make use of. The sector's innate conservatism is evident in how it plans to adapt its approach to data sharing in the future. Though there is an awareness of the need to share through the value chain, as well as a shift in approach, it is still lagging behind every other industry sector we questioned, with 28 per cent of businesses still planning to ringfence their IoT data access to a select few departments in the future.

In terms of the frequency that data is collected in electrical utilities IoT projects, the sector is slightly ahead of the curve when compared to the others we investigated, with 38 per cent of respondents most likely to collect data in real-time. North American organisations are notably further ahead in this area, with 63 per cent likely to collect real-time data in a typical IoT project, while Latin American businesses are lagging, with only 11 per cent committed to real-time data collection. The largest companies also demonstrate a similar commitment to real-time data collection, with 53 per cent of those with over 5,000 employees doing so. It's important for those regions and organisations that are lagging to catch up, as more frequent data collection makes it easier to respond quickly to rapid changes in demand for electricity. Leveraging real-time data from Advanced Metering Infrastructure (AMI), for example, has helped both electricity suppliers and network operators anticipate and respond to the unprecedented fluctuations in demand throughout the Covid-19 pandemic.



At what intervals do you typically gather IoT data points?

- In real-time
- Within half an hour
- Hourly
- Every two hours
- Every four hours (0%)
- Daily



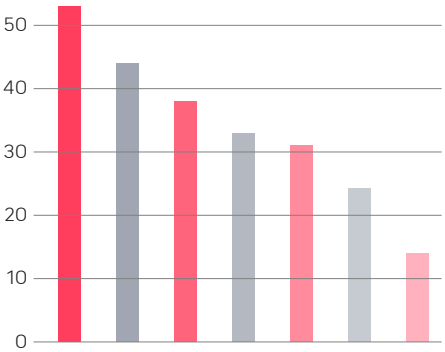
To what extent does/will your organisation share non-sensitive IoT data?

A It is available to anyone in the organisation, or our partners, to access and use

B It is available to anyone in our organisation to access and use

C It is only available to certain departments involved in the IoT project

Currently In the future

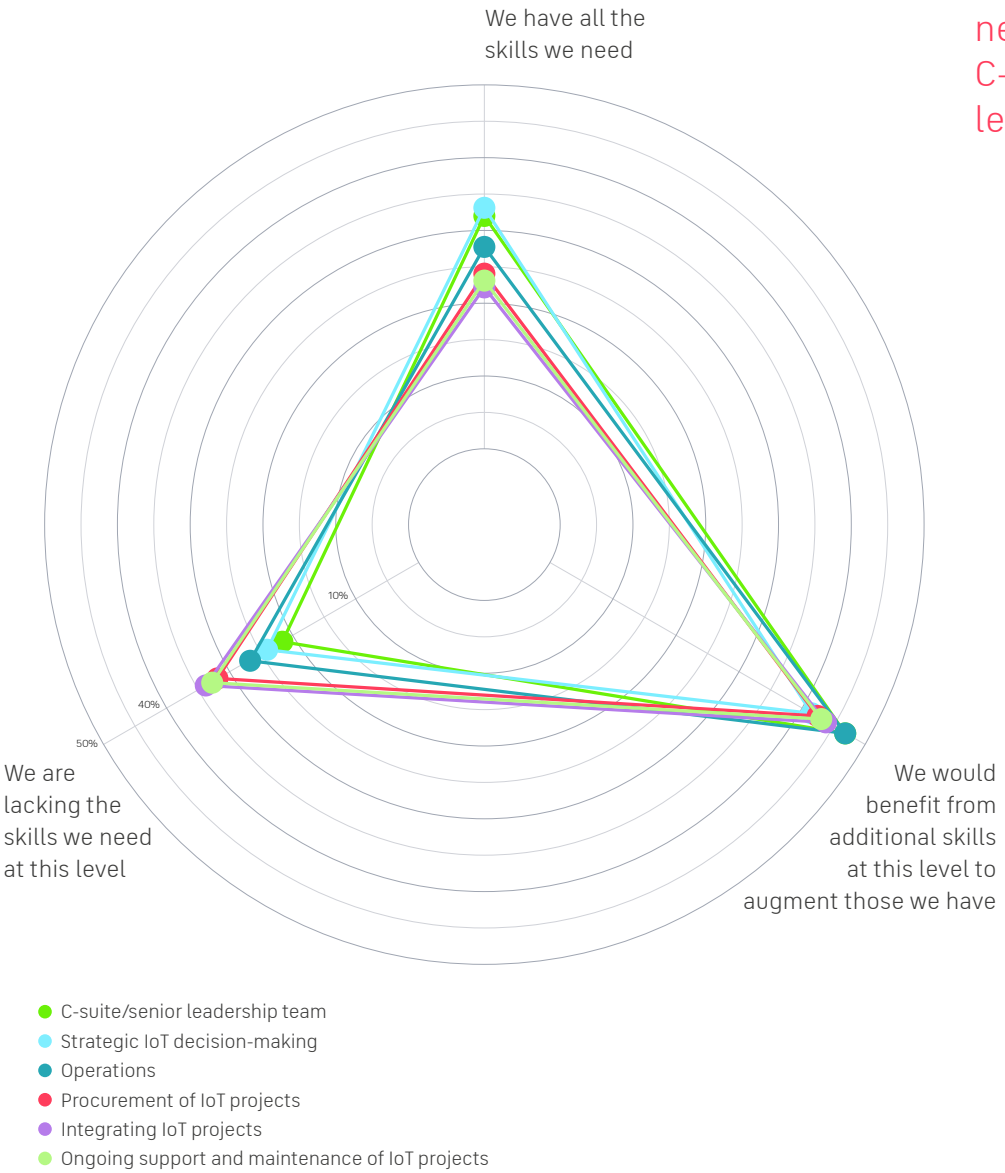


What barriers prevent your organisation from using data optimally?

Security/privacy concerns	53%
Lag between data collection and data being available	44%
Data is stored in an unusable format	38%
Lack of IoT data strategy	33%
We don't have the skills to extract/use data	31%
There is such a large volume of data we struggle to utilise it	29%
We are able to use data as effectively as possible	14%

SKILLS

Does your organisation have the skills needed to fulfil IoT projects at different levels?



"Only a third of all respondents have the necessary IoT skills at the C-suite/ senior leadership level (31 per cent)."

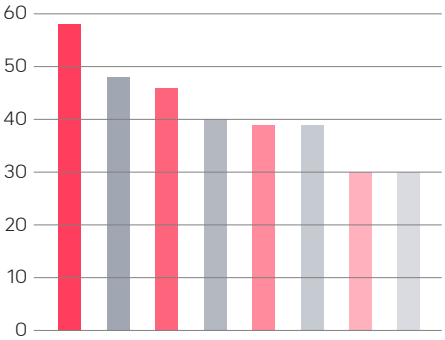
Few electrical utilities organisations have all of the essential skills they need to successfully fulfil their IoT projects at different levels. Only a third (33 per cent) of all respondents have the necessary IoT skills at the strategic IoT decision-making level and only 31 per cent have all the skills they need at the C-suite/ senior leadership level, with the least number of sufficiently skilled workers at the integration level (22 per cent).

While electrical utilities is broadly in line with the sample set in respect to respondents having all the skills they need in each area of the business, it is notable that, amongst larger organisations of over 5,000 employees, 35 per cent are still lacking the skills needed at the senior leadership level and over half (47 per cent) are lacking the skills they need at the strategic IoT decision-making level. Additionally, while both suppliers and network operators are also generally matched when it comes to IoT related skills at most levels, Latin American businesses are severely lagging when it comes to C-suite IoT skills (only 5 per cent) and strategic level skills (0 per cent).

In terms of specific skills that are needed to deliver IoT projects, unsurprisingly for a security conscious sector, security skills are most sought after (cited by 58 per cent). This is followed by analytical/data science skills (48 per cent) and technical support skills (46 per cent). Organisations of over 5,000 employees are also much more likely to seek connectivity technology skills (47 per cent) than the sample (39 per cent). In order to make up for these skills shortages electrical utilities organisations need to work to recruit, upskill or collaborate with trusted service providers or their IoT projects will be hampered.

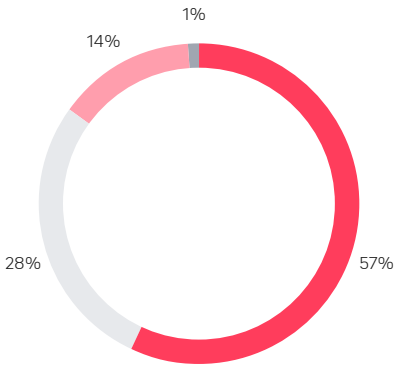
Purchasing decisions around IoT projects in electrical utilities are most likely to come from senior management for network operators (40 per cent) and from the senior leadership team (28 per cent) for energy suppliers. And while there is a reasonably even split between organisations of all sizes when it comes to the levels at which IoT buying decisions are made, there are more senior managers or heads of departments (50 per cent) making these decisions for smaller businesses of 251 to 500 employees.

Well over half of those polled (57 per cent) are aware of off-the-shelf IoT solutions in the marketplace that meet their organisation's needs. A level of awareness that is notably higher is found with larger organisations of 3,001 to 5,000 employees (89 per cent) and for organisations in North America (75 per cent), APAC (71 per cent) and Europe (68 per cent). However, awareness of such solutions amongst respondents in Latin America is extremely low (5 per cent) with 45 per cent noting that providers don't meet their needs at all. Overall, a total of 42 per cent of all respondents in the sector claimed that off-the-shelf utilities IoT solutions only meet some of their needs, or none at all, which highlights the need for service providers to work harder at creating clearer and more cost-effective value propositions.



What additional skills do you need to deliver IoT projects?

Security skills	58%
Analytical/ data science skills	48%
Technical support skills	46%
Project management skills	40%
Strategic skills	39%
Connectivity technology skills	39%
Procurement skills	30%
Database management skills	30%



Are you aware of off-the-shelf IoT solutions that meet your needs?

- Yes, we are aware
- No, providers only meet some of our needs
- No, providers don't meet our needs at all
- Don't know

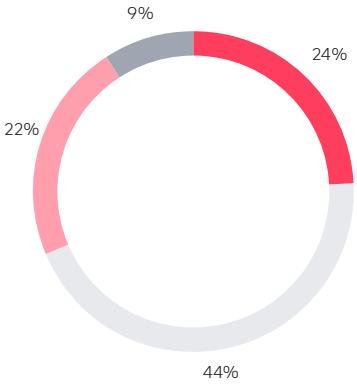
SECURITY

Cyber-security is a key concern for electrical utilities companies because of their place in a nation's critical infrastructure. As electrical organisations leverage IoT to connect power generation, transmission and distribution assets to IT systems, there is an increased risk from cyber-attacks, whether this is from bad actors looking to shut down electricity distribution, or from cyber-criminals looking to extort companies financially.

As such, there are a wide range of security challenges relating to IoT projects that continue to concern electrical utilities organisations, more so in fact than any other sector. The risk of external cyber-attacks is the clear leader in terms of security challenges, with 59 per cent of those surveyed mentioning it as an issue. Additionally, over half of respondents (51 per cent) also list poor network security as a key security challenge associated with the use of IoT projects within their organisation. Insecure storage of data collected is also front of mind (49 per cent), as are internal data regulation and compliance requirements (43 per cent), the misuse of data by employees (42 per cent) and insecure/unencrypted edge networks (41 per cent).

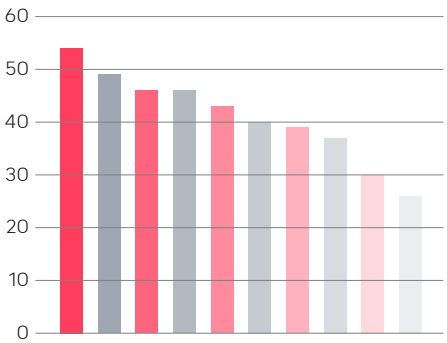
Under a quarter (24 per cent) of all respondents claim that their organisation's IoT solutions have robust cyber-security defences from end-to-end in compliance with the relevant ISO standard. Accordingly, a total of 75 per cent of utilities organisations believe that IoT security needs to be strengthened in some way, with 31 per cent wanting to see major improvements made to their cyber-security defences. The need to see much improved defences increases considerably for those organisations in Russia (90 per cent) and Latin America (89 per cent).

The positive news is that the sector is largely taking a proactive approach to tackle these various security concerns, with 54 per cent of respondents having already created an internal IoT security policy, 49 per cent hiring skilled staff and 46 per cent training employees on IoT and upgrading existing security technologies. North American utilities organisations are ahead of the curve on IoT security, with 71 per cent training employees on IoT and 67 per cent upgrading existing security technology and having created an internal IoT security policy.



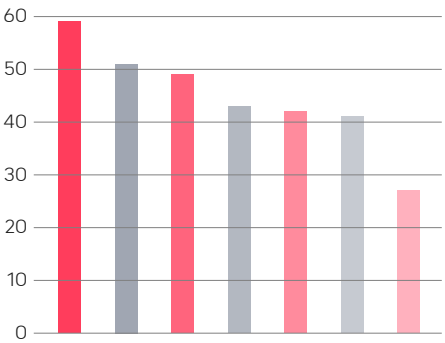
Which of the following statements are accurate regarding the security of your IoT projects?

- We have robust cyber-defences
- Our defences are good but could be stronger
- We need much better cyber-defences
- Our cyber-defences need to be vastly improved



What changes have you made to address IoT security concerns?

- Creation of an internal IoT security policy 54%
- Hiring skilled staff 49%
- Upgrading existing security technologies 46%
- Training employees on IoT 46%
- Investing in new security technologies 43%
- Communicating to customers on the use of IoT 40%
- Partnering with a third party 39%
- Creation of an external IoT security policy for suppliers and partners 37%
- Securing physical assets such as sensor nodes 30%
- Implementing a backup connectivity network 26%



What are your biggest IoT security challenges?

- Risk of external cyber-attack 59%
- Poor network security 51%
- Insecure storage of data collected 49%
- Internal data regulation and compliance requirements 43%
- Potential mishandling/misuse of data by employees 42%
- Insecure/unencrypted edge networks 41%
- Supplier/partner data regulation compliance requirements 27%

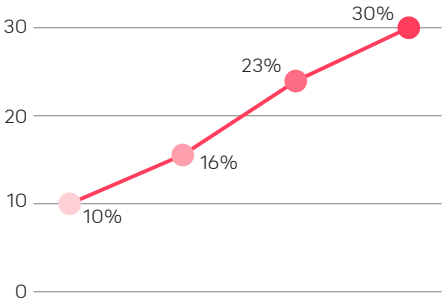
INVESTMENT

IoT budgets for the electrical utilities sector are higher than most of the other sectors we surveyed (other than oil and gas), with an average planned spend on IoT projects in the next three years of $3,101,705, which represents 10 per cent of the annual IT budget. This is slightly higher than the sample average of $2,804,899. As you would expect, IoT budgets also tend to be higher in larger organisations, rising to $3,789,167 for companies with between 1,000 and 3,000 employees, and to $3,703,125 for those with more than 5,000.

The sector's level of IoT maturity is reflected in the fact that the proportion of their IT budget allocated for IoT projects over the next three years (9.9 per cent) is equal to that for cloud computing (9.9 per cent) and higher than that for all other digital transformation technologies, including next generation security (8 per cent), big data analytics (8 per cent), augmented/virtual reality (5 per cent), machine learning (5 per cent) and robotics (5 per cent).

Despite the maturity of IoT adoption and the clear business benefits that IoT projects are already having on energy generators and network operators, this commitment to continuing high levels of investment throughout the sector suggests a clear IoT roadmap is in place in the majority of respondent organisations.

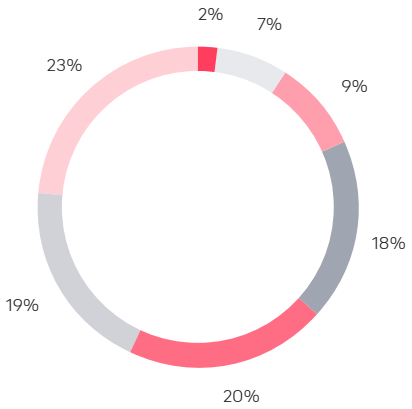
Finally, the most positive sign of all that IoT is impacting the bottom line is reflected in the high levels of awareness of how IoT engagement can save the business money in both the short and long term. Currently, the average estimated costs saved for businesses from IoT projects across the sector is 10 per cent, with this expected to rise to 16 per cent in 12 months, before eventually reaching 30 per cent in five years. These projected cost savings are at their highest for organisations in Europe (36 per cent), North America and APAC countries (both 33 per cent).



What proportion of your organisation's costs are saved/going to be saved from IoT projects?

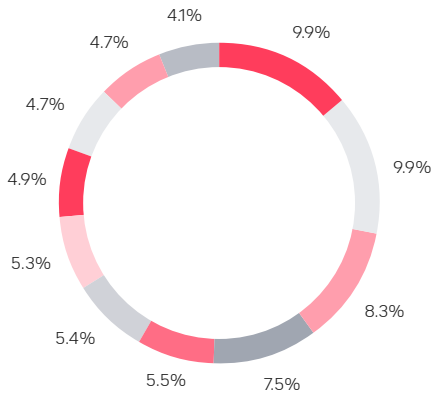
Currently	10%
In 12 months	16%
In 3 years	23%
In 5 years	30%

"The proportion of electrical utilities organisations' IT budget allocated for IoT projects over the next three years (9.9 per cent) is equal to that for cloud computing (9.9 per cent)."



What is your planned investment in IoT projects in the next three years?

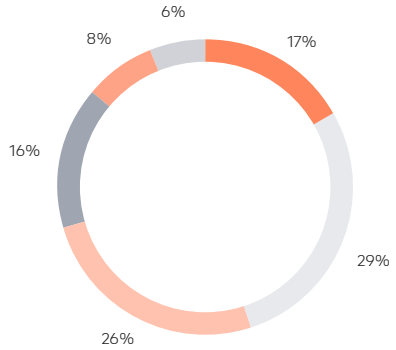
- $0 to £100,000
- $100,000 to $500,000
- $500,000 to $1,000,000
- $1,000,000 to $2,000,000
- $2,000,000 to $3,000,000
- $3,000,000 to $4,000,000
- $4,000,000 and above



What proportion of your IT budget will you spend on IoT projects in the next three years?

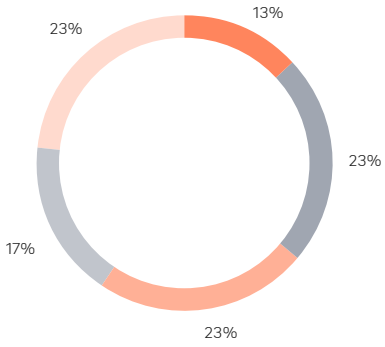
- IoT projects
- Cloud computing
- Next generation security
- Big data analytics
- Machine Learning
- Robotics
- Augmented Reality
- Virtual Reality
- Cognitive AI
- Blockchain
- 3D Printing

MINING



Respondents by sub-sector (%)

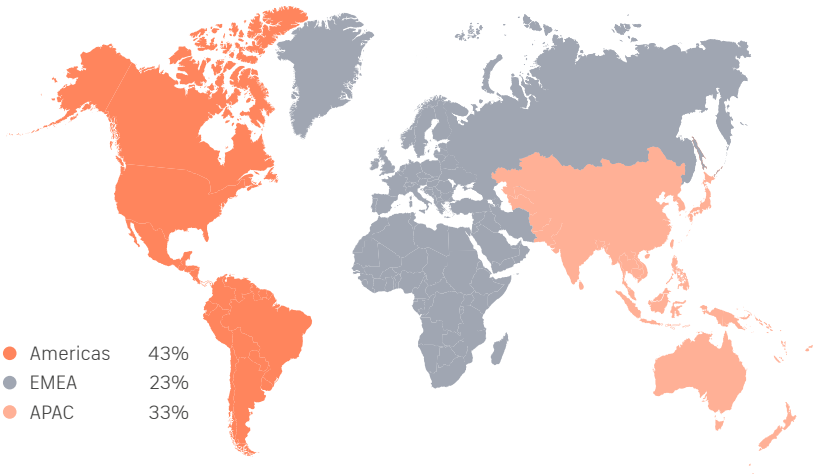
- Multi-commodity
- Iron ore
- Copper
- Gold
- Other bulk minerals
- Other



Respondents by size of organisation (%)

- 251-500 employees
- 501–1,000 employees
- 1,001–3,000 employees
- 3,001–5,000 employees
- More than 5,000 employees

Respondents by region (%)



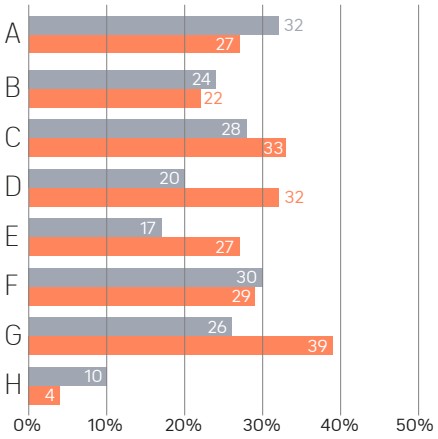
Americas	43%
EMEA	23%
APAC	33%

The need to extract raw materials in safer, more efficient, sustainable and cost-effective ways is driving the adoption of Industry 4.0 technologies across the global mining sector. Even aside from the far-reaching impact of Covid-19, it is evident mining companies are facing a slew of challenges: pricing volatility, supply chain issues, a shifting regulatory landscape, as well as societally driven changes in investor behaviour.

In early 2020 McKinsey suggested Covid-19 slowing global industrial output would lead to a decline in demand for those metals used principally for industrial and construction use cases, such as aluminium, zinc, and iron ore. On the other hand they predicted the price of countercyclical minerals such as gold and those with new industry use cases such as copper, lithium and graphite would remain more resilient.[1] These predictions have largely come to pass, and while parts of the world are returning to a new normal, industry is suppressed in many others, causing demand for metals to remain below where it was in 2019.

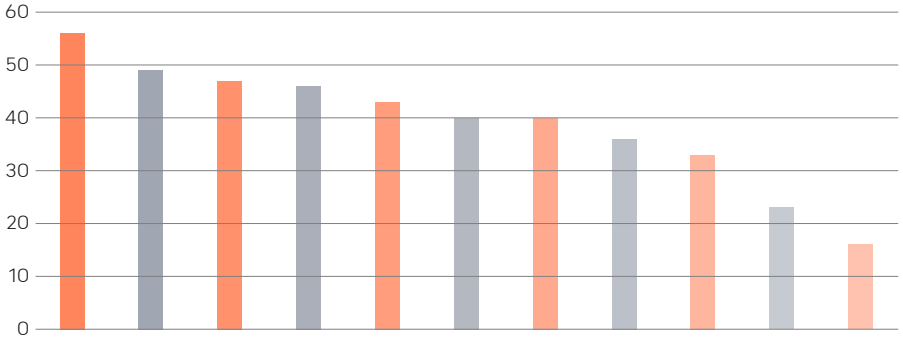
On the supply side there has been a global reduction in the amount of available commodities due to restrictions on movement. The impact of Covid on a country and its response, has in many ways dictated the fate of its mining operations, with countries responsible for much of the world's output in certain metals experiencing mixed fortunes. In some cases whole operations have ground to a halt and supply chains have had to adapt and seek alternatives with varying levels of success. In example, manufacturers of semiconductors were notably affected because of a reduction in available rare earths.

"The impact of Covid on a country has in many ways dictated the fate of its mining operations, with countries responsible for much of the world's output in certain metals experiencing mixed fortunes."



What barriers, if any, does your organisation face in the deployment of IoT projects?

- A Lack of consistent and reliable connectivity
- B Lack of available capital to invest in IoT projects
- C A lack of in-house skills
- D Lack of turnkey/off-the-shelf solutions
- E IoT not being prioritised by the board
- F Security implications
- G Integrating IoT technology with existing platforms
- H Not encountered any barriers at this stage
- Encountered in the deployment phase
- Encountered/expect to encounter this once deployed



What are the most important drivers for the deployment of IoT projects for your organisation?

Improve environmental sustainability	56%	Reduced downtime	40%
Better decision-making	49%	Greater supply chain insight	36%
Increase staff productivity	47%	Improve customer experience	33%
Cost efficiencies	46%	New revenue streams	23%
Greater automation	43%	Lower insurance premiums	16%
Improve health and safety	40%		

[1] https://www.mckinsey.com/industries/metals-and-mining/our-insights/lessons-from-the-past-informing-the-mining-industrys-trajectory-to-the-next-normal

How the industry rebounds in the coming years will depend to some extent on its use of Industry 4.0 technologies to overcome supply chain obstacles. Already we are seeing evidence that those companies that are increasing the speed of adoption of the Internet of Things (IoT) and associated technologies are gaining an advantage, through their ability to maintain operations autonomously and with greater insight.

Nearly half (47 per cent) of all mining respondents in our research noted that the challenges of Covid-19 have demonstrated the importance of the Internet of Things (IoT) and automation to ensure the continuing success of their business. The pandemic has accelerated the rate of IoT adoption in many mining businesses, with 40 per cent of respondents having already accelerated deployments of their IoT projects in response to the challenges of the pandemic, and 41 per cent intending to start accelerating within the next few years.

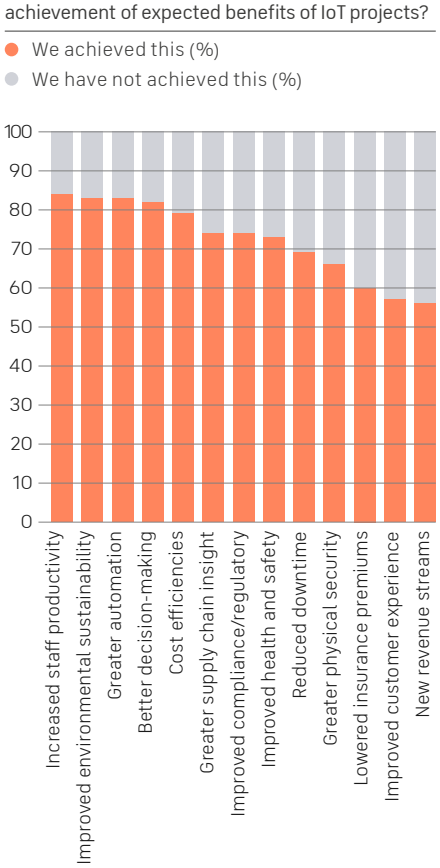
While the mining sector has, historically, lagged behind other industries in its adoption of radical ideas and new technologies, our research also reveals that the sector has made considerable progress in terms of IoT adoption and development over the last few years and is upbeat about its potential. While progress has been made in mining IoT adoption globally, the North American miners are currently leading the way with the highest investment commitments on IoT spending.

IoT is helping miners improve safety, environmental sustainability, informing better decision making and increasing both productivity and cost-savings across the entire value chain. From automating haulage vehicles and monitoring drilling through to closely monitoring environmental conditions, vehicle telemetry, machinery and tailings dams, the industry is rapidly increasing its investments in IoT projects, with most respondents in our research already achieving the expected benefits in these key areas.

Key to organisations unlocking the potential of IoT is a formal IoT strategy, which 46 per cent of our mining respondents stated they have. There are regional variations in levels of IoT maturity: while 53 per cent of mining companies in APAC have a formal IoT strategy, this drops to only 37 per cent of Latin American businesses.

With a rapid increase in IoT adoption over 2020 the mining industry is reaching new levels of IoT maturity, but there are still challenges to overcome. Connectivity challenges, particularly in relation to reliable connectivity for mobile assets, persist and businesses need to look at the right blend of technologies from their service providers to move projects from trial to full implementation more easily. Skills, particularly around technical support and integration need to be bolstered. The industry is also highly security aware and, encouragingly, is taking steps to improve its defences, with over half (56 per cent) of all respondents investing in new technologies to address IoT security concerns, more so than any other sector we surveyed.

How would you score your organisation's achievement of expected benefits of IoT projects?



ADOPTION

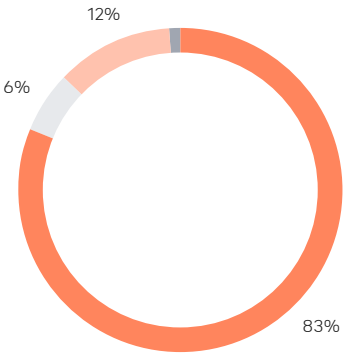
Most organisations in the mining sector (83 per cent) have now fully deployed at least one IoT project, a considerable increase since our 2018 research, when a different sample set indicated only 2 per cent had fully deployed. 37 per cent of respondents have deployed within the last 12 months, which shows a rapid acceleration in IoT adoption across the sector throughout 2020. This clearly displays how the mining industry is fast approaching a level of maturity and is no longer lagging behind other industries. The rapid acceleration in adoption can be further contextualised by the 40 per cent who stated that challenges related to Covid-19 has accelerated their adoption of IoT.

The drivers motivating mining businesses to deploy IoT projects are also a clear reflection of the numerous challenges faced by the sector. Improving environmental sustainability is cited as the most popular reason by 56 per cent of respondents. Followed by better decision-making (49 per cent), increased staff productivity (47 per cent), cost efficiencies (46 per cent), greater automation (43 per cent) and improved health and safety (40 per cent). Better decision-making was viewed as the most important driver of IoT usage in North America (65 per cent), while in APAC it was increased staff productivity and in Latin America it was improved environmental sustainability (both 63 per cent).

In terms of use cases the most common area IoT is being engaged is in automated haulage vehicles, where 28 per cent of respondents have already deployed IoT solutions, and an additional 23 per cent are in the trial phase. Drill monitoring was in second place with 27 per cent of respondents closely followed by monitoring environmental conditions (26 per cent), vehicle telemetry monitoring (24 per cent), machinery monitoring and control (23 per cent) and monitoring tailings facilities or shipment/supply chain tracking (both 22 per cent).

Over the next couple of years, our sample expects to see an increase in fully deployed IoT projects focused on machinery monitoring and control. 46 per cent of respondents are currently trialling these projects, as well as projects focused on monitoring tailings facilities and environmental conditions (currently being trialled by 42 per cent and 41 per cent, respectively). Larger organisations of 3,001 to 5,000 employees are ahead of the curve in these last two areas, with 67 per cent of respondents currently trialling these projects. The most likely use cases to fail in the trial stage were automated haulage vehicles (23 per cent) and vehicle telemetry monitoring (19 per cent) suggesting there may be connectivity challenges related to mobile assets.

Despite the significant progress being made in the areas outlined above, there are still a number of barriers that need to be overcome in order for mining organisations to unlock more value from their IoT projects. During the deployment phase, 32 per cent of organisations were challenged by the lack of consistent and reliable connectivity, closely followed by security implications (30 per cent) and a lack of in-house skills (28 per cent). The number of respondents indicating that connectivity was a barrier to optimal IoT deployment was higher in mining compared to the other sectors we interviewed.



What is your current status in terms of deploying IoT projects?

- Fully deployed
- Currently trialling
- Planning to trial within 12 months
- Planning to trial in 18 months – 2 years

Once projects are deployed respondents indicated that the biggest barriers were the ability to integrate IoT technology with existing platforms (39 per cent), a lack of in-house skills (33 per cent) and a lack of turnkey/off-the-shelf solutions (32 per cent). Connectivity also remains a key barrier post-deployment for nearly half (48 per cent) of mid-sized mining organisations.

Finally, most mining organisations have already achieved the expected benefits of IoT projects in a range of key areas. 84 per cent of respondents in the sector have achieved increased staff productivity, closely followed by improved environmental sustainability and greater automation (83 per cent), better decision-making (82 per cent), cost efficiencies (79 per cent), greater supply chain insight (74 per cent) and improved health and safety (73 per cent).

What IoT projects has your organisation already deployed and what will your organisation deploy in the future?

CONNECTIVITY

IoT is essentially a network of networks and is dependent on reliable connectivity for its successful application. With many mining sites located in remote and often harsh environments, spread over great distances with varied and often changing topology, the sector faces its own very specific connectivity challenges. For these reasons, accessing and using the right kinds of connectivity technologies, continues to be a major barrier to IoT adoption in the mining sector.

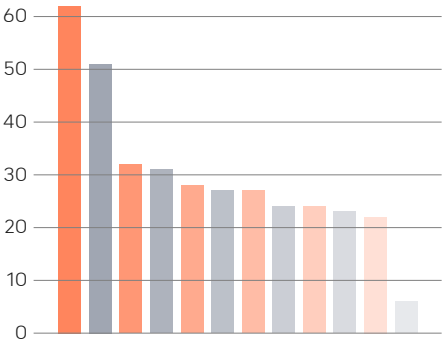
Only 28 per cent of mining organisations consider public terrestrial networks (such as cellular or fibre) to be suitable for the connectivity they need to deploy IoT projects. This explains why satellite is by far the most widely used type of long-range connectivity used in mining IoT projects (62 per cent), a noticeably higher proportion than all other industry sectors in our research. In-fact 97 per cent of respondents stated that satellite connectivity provides crucial support to their organisation's IoT communication networks.

In addition to satellite, mining respondents employ a wide range of other connectivity types in their IoT projects, combining both short- and long-range technologies with three types used on average, similar to the average across all sectors. In terms of edge connectivity Wi-Fi is still the most popular short-range connectivity type (32 per cent), despite its limitations in terms of range and power consumption. LPWAN technologies are also becoming increasingly popular as they are highly suitable for connecting large numbers of data producers, with LoRaWAN used by 27 per cent of respondents.

Even so, connectivity issues continue to thwart the successful rollout of IoT projects, with the majority (63 per cent) of mining respondents struggling to deploy IoT because they have connectivity issues in the areas they want to deploy it. A notably high proportion (92 per cent) encounter connectivity challenges in the trial or proof of concept phase of their projects and 68 per cent continue to experience disruption after deployment, which raises questions around the suitability of their connectivity solution. 83 per cent agree that their IoT projects have enjoyed much more success since solving their connectivity challenges.

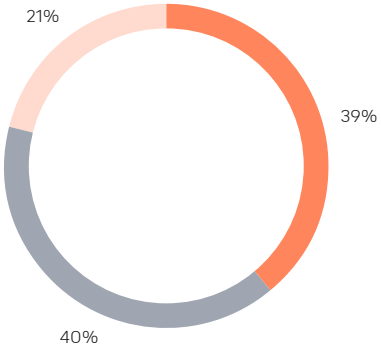
When making a choice on connectivity type, mining respondents indicated a range of preferences in the qualities they required, with reliability the most cited (51 per cent), followed by low latency (41 per cent), bandwidth (40 per cent) and cost (33 per cent). The requirement for highly reliable connectivity was more prominent in mining than any other industry surveyed.

As mining sites are very often based in remote areas away from terrestrial communications, there will often be instances where comms outages occur. That is why it is vital for mining companies to use a backup connectivity method to avoid potentially losing mission critical data. However, only 39 per cent of our mining respondents indicated that they use such a backup connection type to continue collecting data in the event of an outage. A further 40 per cent indicated that their operations would go offline, and 21 per cent will pause all data collection completely until the original connection is restored, leading to the loss of highly valuable data and potentially revenues. Larger miners (57 per cent) and North American miners (55 per cent) are more likely to use backup connections than rely on offline data collection or pausing the process.



What connectivity types does your organisation use in its IoT projects?

Satellite	62%
Radio	51%
Wi-Fi	32%
Cellular (private)	31%
Cellular (public)	28%
LoraWAN	27%
NB IoT	27%
Bluetooth Low Energy (BLE)	24%
Sigfox	24%
Zigbee	23%
Fibre	22%
Other	6%



In remote areas away from terrestrial communication, what do you do if unable to connect to your chosen connectivity type.

- Use a backup connection type to continue
- Continue collecting data offline until the connection is restored
- Pause all data collection until connection is restored

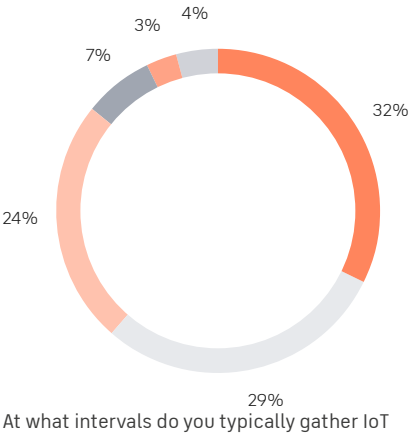
DATA

It is vital that the data that mining companies are producing in their IoT projects can be used to provide actionable business insights. To optimise such insights, data needs to be delivered at the right time and in the right format to the right people. The mining professionals we surveyed listed several hurdles to effective data management which they regularly face, with security and privacy concerns the most prominent at 49 per cent, followed by a lag between data collection and availability at 48 per cent. Security concerns and data lag issues are even more prominent for Latin American mining organisations (58 per cent and 74 per cent respectively) than the sector as a whole.

Following those primary hurdles to effective data collection, the lack of an IoT data strategy was problematic for 34 per cent of mining respondents. Without an effective IoT data strategy in place, mining companies will struggle to govern the flow of data, both inside and outside their organisation. In terms of data sharing, miners are clearly adopting a progressive Industry 4.0 mind-set with 43 per cent making data available to anyone in the organisation, and an additional progressive 23 per cent also open to sharing this data with partners. Still, a third of our respondents currently restrict access to this data to departments directly involved in IoT projects, correlating with the above-mentioned group that don't yet possess a data strategy.

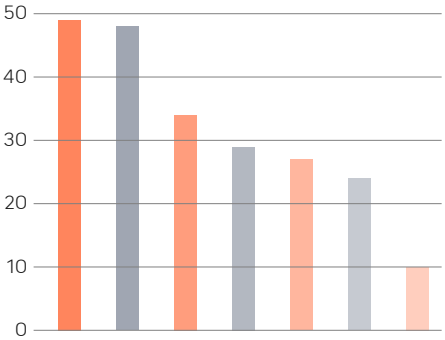
In the future, mining organisations will increasingly share their data, with 40 per cent of respondents indicating they plan to make data available to partners and external parties and only 17 per cent planning to continue ring-fencing access to data to selected departments. This clear trend towards data sharing and a culture of collaboration is an encouraging sign, as it will help the mining supply chain optimise operations more effectively.

When looking at the frequency that data is collected in mining IoT projects, the mining sector is slightly ahead of the curve, compared to some of the others that we investigated, with the majority (32 per cent) employing real-time data collection, compared to the wider sample average of 30 per cent. Many mining businesses are also likely to collect data every half an hour (29 per cent), although hourly collection (24 per cent) is also a common approach. North American respondents and the largest mining organisations (over 5,000 employees) are noticeably more advanced when it comes to using real-time data collection, at 40 per cent and 43 percent, respectively. It's important that smaller mining businesses and those in other regions start to investigate real-time data collection to get the most value from their IoT projects.



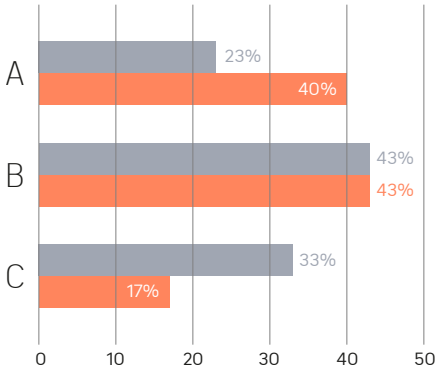
At what intervals do you typically gather IoT data points?

- In real-time
- Within half an hour
- Hourly
- Every two hours
- Every four hours
- Daily



What barriers prevent your organisation from using data optimally?

Security/privacy concerns	49%
Lag between data collection and data being available	48%
Lack of IoT data strategy	34%
We don't have the skills to extract/use data	29%
Data is stored in an unusable format	27%
There is such a large volume of data we struggle to utilise it	24%
We are able to use data as effectively as possible	10%



To what extent does/will your organisation share non-sensitive IoT data?

A It is available to anyone in the organisation, or our partners, to access and use

B It is available to anyone in our organisation to access and use

C It is only available to certain departments involved in the IoT project

Currently In the future

SKILLS

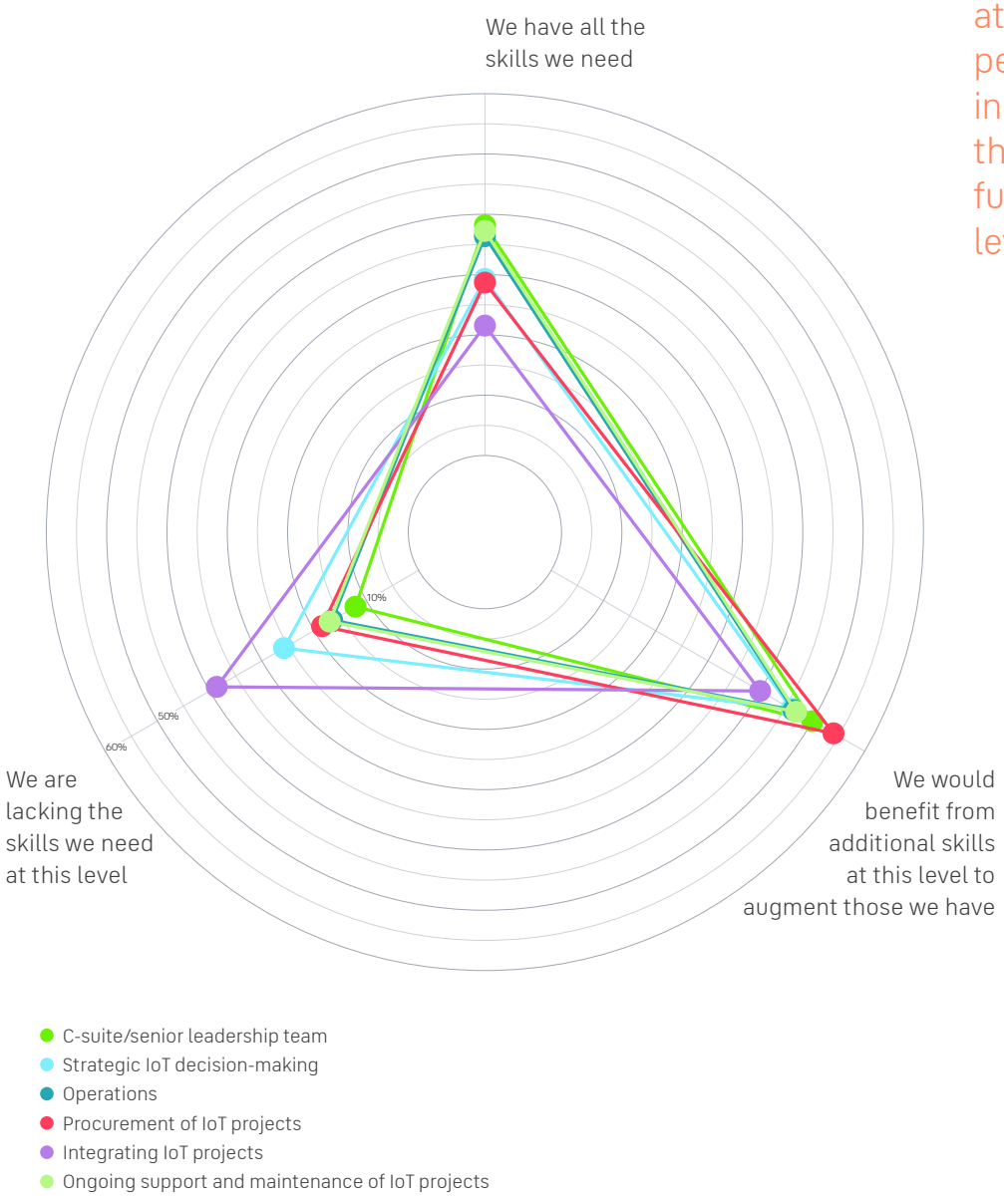
In addition to a lack of consistent and reliable connectivity, one of the biggest hurdles to successful IoT adoption is a lack of the right skillsets, with a third of mining respondents either having already encountered or expecting to encounter a lack of in-house skills as a barrier to the deployment of IoT projects. This is a problem that businesses need to resolve, either by hiring, upskilling, or working with a service provider.

The most skilled personnel were found at C-suite level, with 38 per cent of respondents indicating they have all the skills they need to fulfil IoT projects at that level. That C-suite leadership is so well thought of within the sector is suggestive of the journey that mining has been on to bring in new digital talent from other sectors.

Our respondents indicated that the level they most lacked the skills in was around the integration of IoT projects, with 38 per cent lacking the skills needed and only 22 per cent stating they have all the skills they need to do this effectively. It is clear that mining organisations need to upskill in this area, to effectively integrate newer technologies and connectivity methods with legacy systems.

"Overall, the most skilled personnel were found at C-suite level, with 38 per cent of respondents indicating they have all the skills they need to fulfill IoT projects at that level."

Does your organisation have the skills needed to fulfil IoT projects at different levels?

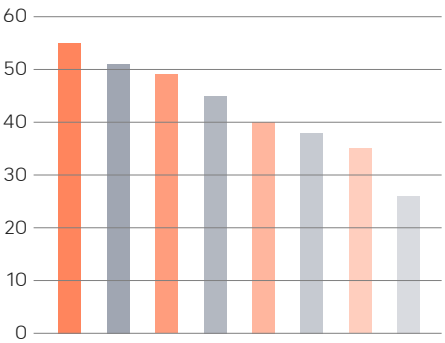


The survey results highlight a lack of strategic decision-making skills (26 per cent), although a slightly higher proportion (29 per cent) of the respondents did state that they had all the skills they needed here. The lack of strategic decision making and integrating IoT projects skills was most keenly felt in Latin America, with 63 per cent and 68 per cent respectively lacking the skills they need in these areas.

To address skills deficiencies, technical support skills are most sought after (cited by 55 per cent), followed by connectivity technology skills (51 per cent), analytical and data science skills (49 per cent) and security skills (45 per cent). A high proportion (62 per cent) of respondents from the largest organisations we surveyed specifically cited a need for additional connectivity skills to deliver their IoT projects.

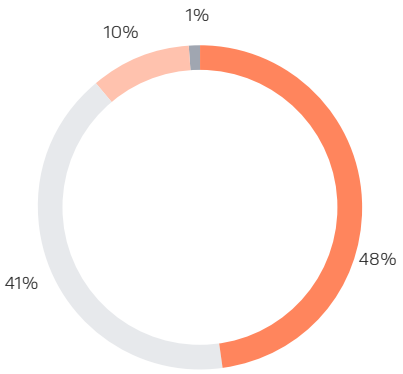
Most purchasing decisions around IoT projects are made at the senior management level, such as heads of departments in mining companies (53 per cent). Although C-suite executives (22 per cent) and middle managers (20 per cent) are also involved. IoT purchasing decisions at larger organisations with over 5,000 employees are more likely to be made at C-suite level (29 per cent) and less likely to be made by middle management (14 per cent).

Just under half of those polled (48 per cent) are aware of off-the-shelf IoT solutions in the marketplace that help them meet their organisation's needs. This figure increases to 73 per cent for those larger organisations of 3,001 to 5,000 employees. However, there is still a total of 51 per cent of all mining respondents believing that external IoT solutions providers either only meet some of their needs or, worse, meet none of them at all. This indicates that there is still a way to go for solution providers to improve their mining industry offerings and build better connections with mining companies.



What additional skills do you need to deliver IoT projects?

Technical support skills	55%
Connectivity technology skills	51%
Analytical/ data science skills	49%
Security skills	45%
Project management skills	40%
Procurement skills	38%
Strategic skills	35%
Database management skills	26%



Are you aware of off-the-shelf IoT solutions that meet your needs?

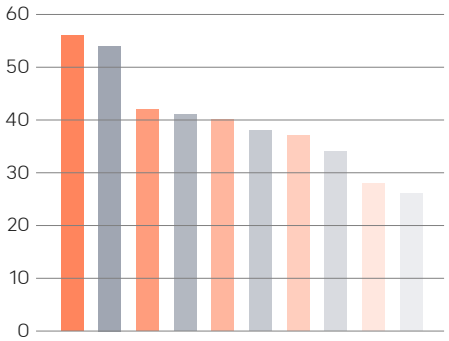
- Yes, we are aware
- No, providers only meet some of our needs
- No, providers don't meet our needs at all
- Don't know

SECURITY

Security breaches are a huge concern for mining companies: partly because of their significant geo-political status, but also due to the value of their commercial data. And with mining companies increasingly connecting their operational infrastructure to the internet with IoT projects, it is no surprise that over half (54 per cent) of all respondents in the sector cite the risk of external cyber-attacks as the biggest security challenge associated with the use of IoT in their organisation.

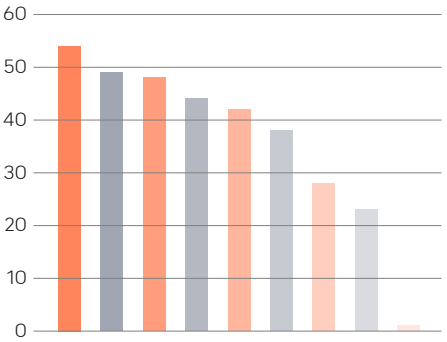
Other key security challenges across the mining sector include insecure or unencrypted edge networks (49 per cent), internal data regulation and compliance requirements (48 per cent), insecure storage of collected data (44 per cent) and poor network security (42 per cent). Mining organisations in Latin America are particularly concerned about the risk of cyber-attacks and poor network security, with 68 per cent of respondents from the region citing these as the two biggest security challenges they face.

Overall, 74 per cent of all mining respondents believe their IoT defences could be more robust, with 12 per cent noting that cyber-security defences have not been a priority for their organisation and could be vastly improved. Encouragingly mining is slightly ahead of the curve, with over a quarter (26 per cent) stating that their organisation's IoT solutions have robust cyber-security defences from end-to-end in compliance with the relevant ISO standard.
The good news is that the mining sector is taking positive action to respond to perceived cyber-security threats, with over half (56 per cent) of respondents investing in new security technologies, creating an internal IoT security policy (54 per cent), creating an external IoT security policy for suppliers and partners (42 per cent) or training employees on IoT security (41 per cent). 67 per cent of those working in the largest organisations (over 5,000 employees) are particularly focused on the creation of an internal IoT security policy. Elsewhere a notably higher proportion of Latin American respondents (68 per cent) are investing in new security technologies.



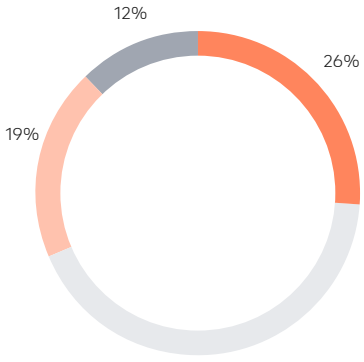
What changes have you made to address IoT security concerns?

Investing in new security technologies	56%
Creation of an internal IoT security policy	54%
Creation of an external IoT security policy for suppliers and partners	42%
Training employees on IoT	41%
Partnering with a third party	40%
Upgrading existing security technologies	38%
Communicating to customers on the use of IoT	37%
Securing physical assets such as sensor nodes	34%
Hiring skilled staff	28%
Implementing a backup connectivity network	26%



What are your biggest IoT security challenges?

Risk of external cyber-attack	54%
Insecure/ unencrypted edge networks	49%
Internal data regulation and compliance requirements	48%
Insecure storage of data collected	44%
Poor network security	42%
Potential mishandling/misuse of data by employees	38%
Insecure storage of data collected	28%
Supplier/partner data regulation compliance requirements	23%
Don't know	1%



Which of the following statements are accurate regarding the security of your IoT projects?

- We have robust cyber-defences
- Our defences are good but could be stronger
- We need much better cyber-defences
- Our cyber-defences need to be vastly improved

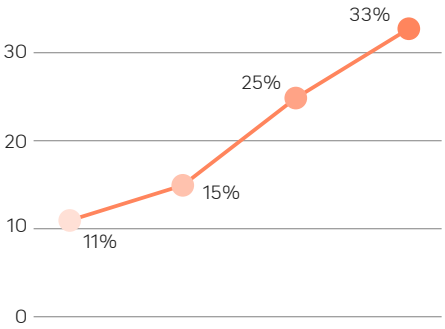
INVESTMENT

The average investment in IoT projects per organisation in the mining sector is estimated to be $2,729,444 over the next three years. A further 20 per cent of mining respondents are expecting to spend more than $4,000,000 on IoT in the same timeframe. As would be expected, smaller mining organisations have a lower planned spend than the average, while the biggest companies plan to invest the most (an average of $4,264,286 for those with more than 5,000 employees).

Despite these differences in planned IoT investments in terms of size, it is clear that IoT is being prioritised in IT budgets, exceeding the spend on cloud computing, big data analytics, next generation security or machine learning over the next three years. This trend is particularly evident in North America, where 11.8 per cent of budgets will be spent on IoT in the next three years.

While European-based mining organisations are slightly behind the investment curve, only allocating 8.9 per cent on IoT, preferring to invest more in other technologies such as machine learning, cognitive AI and blockchain.

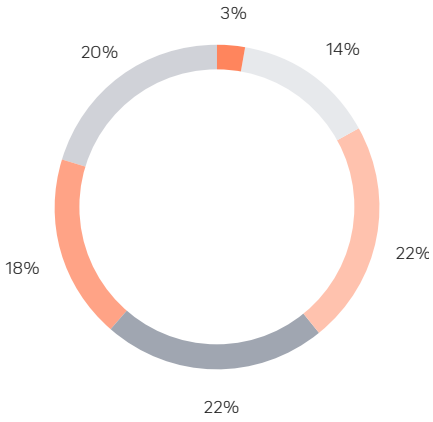
Mining respondents also display a clear awareness of the potential for IoT to save their businesses money, both in the short and long term. Currently, the average estimated proportion of an organisation's cost saved is 11 per cent, with this expected to rise to 15 per cent in 12 months, before eventually reaching 33 per cent in five years. This final figure highlights the optimism for IoT technology in the sector. Larger organisations with over 5,000 employees expect to see even greater savings in the long term, expecting an average of 36 per cent in five years.



What proportion of your organisation's costs are saved/going to be saved from IoT projects?

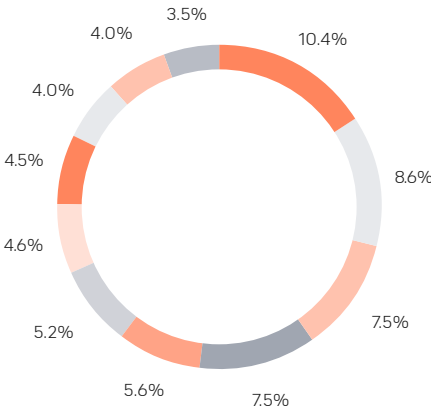
Currently	11%
In 12 months	15%
In 3 years	25%
In 5 years	33%

"The average investment in IoT projects per organisation in the mining sector is estimated to be $2,729,444 over the next three years."



What is your planned investment in IoT projects in the next three years?

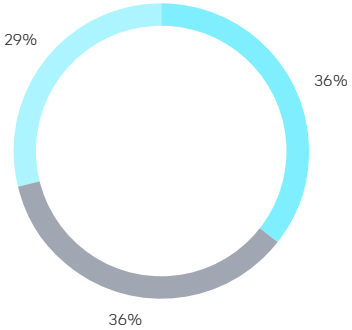
- $100,000 to $500,000
- $500,000 to $1,000,000
- $1,000,000 to $2,000,000
- $2,000,000 to $3,000,000
- $3,000,000 to $4,000,000
- $4,000,000 and above



What proportion of your IT budget will you spend on IoT projects in the next three years?

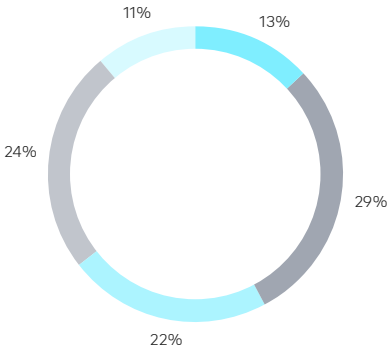
- IoT projects
- Cloud computing
- Big data analytics
- Next generation security
- Machine Learning
- Augmented Reality
- Cognitive AI
- Virtual Reality
- 3D Printing
- Blockchain
- Robotics

OIL AND GAS



Respondents by sub-sector (%)

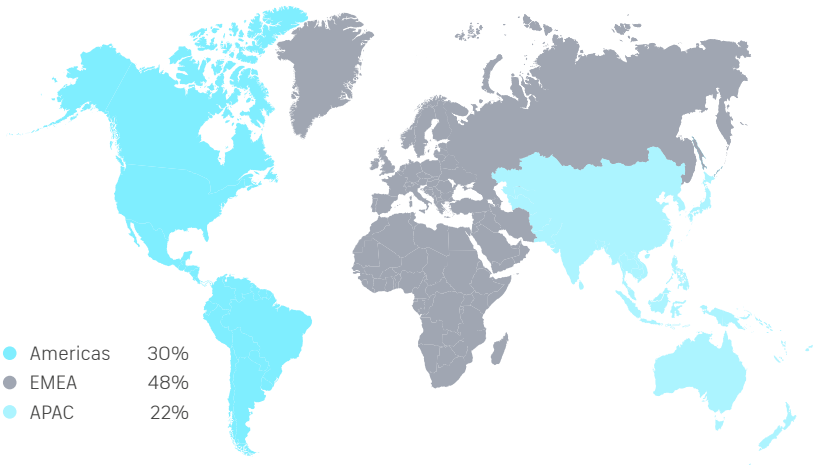
- Exploration
- Extraction
- Distribution



Respondents by size of organisation (%)

- 251-500 employees
- 501–1,000 employees
- 1,001–3,000 employees
- 3,001–5,000 employees
- More than 5,000 employees

Respondents by region (%)



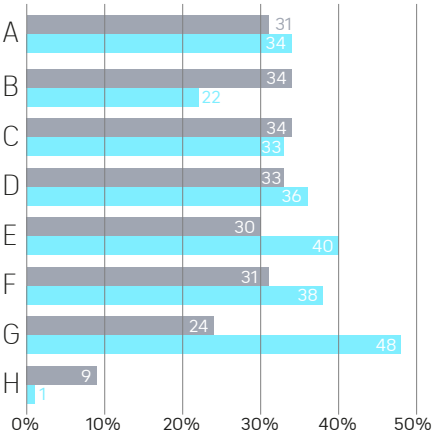
- Americas 30%
- EMEA 48%
- APAC 22%

The oil and gas sector has fuelled industry, travel and virtually every other aspect of global economic and social activity for over a century, but faces the most challenging period of its existence. According to Deloitte; 'global oil demand fell by 25 per cent in April [2020]' due to the Covid-19 pandemic, and while it has rebounded it will remain below pre-Covid levels.[1] This vision of the future can partly be attributed to behavioural changes rendered on the world by Covid, which continue to impact our lives, although it is also the result of a macro-shift toward more sustainable fuel sources such as nuclear, hydro, solar and wind power.

While parts of the world are reducing their reliance on hydrocarbons, other areas will continue to rely heavily on them, and the industry will continue to be a significant economic force irrespective of the pressures it currently faces. To succeed in the face of this pressure, the sector will have to innovate and is likely to see some consolidation as a result. The good news is the oil and gas sector has a history of innovation and has been moving head-on to meet these challenges for a while, though the pace and investment to adopt these technologies has now increased due to the pandemic. Those companies that best utilise technologies to optimise their operational models will carve out profitable paths in the years ahead.

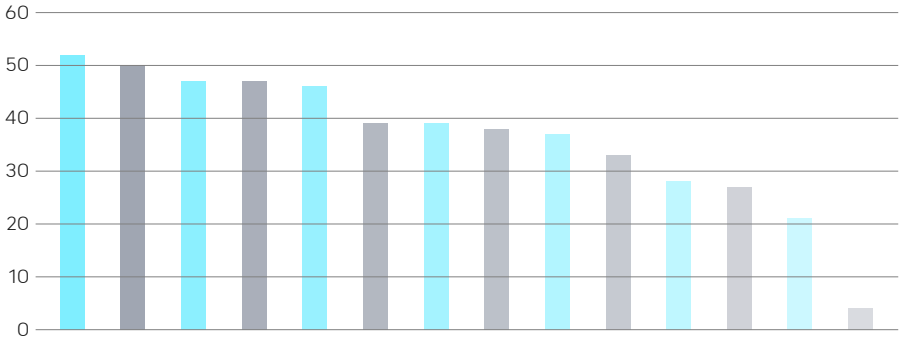
Even without Covid, there are numerous challenges facing the sector at all stages of the value chain. Within the last decade, technology advances have made it possible to unlock more oil from old fields. At the same time, higher oil prices have made it economical for companies to go after reserves that are harder to reach. Businesses exploring new sites are faced with the challenge of more inaccessible, unsafe locations to work in, leading to organisations harnessing automated technology to make data driven decisions quickly and efficiently. Once production sites have been established, extractive processes need to be sharpened to be as efficient as possible to maximise profits, with efficiencies particularly important while supply outstrips demand. Midstream distributors transporting oil and gas through pipelines also need to work out ways to deliver as much product as possible, without leakage or incident.

"Extractive processes need to be sharpened to be as efficient as possible to maximise profits."



What barriers, if any, does your organisation face in the deployment of IoT projects?

- A Lack of consistent and reliable connectivity
- B Lack of available capital to invest in IoT projects
- C A lack of in-house skills
- D Lack of turnkey/off-the-shelf solutions
- E IoT not being prioritised by the board
- F Security implications
- G Integrating IoT technology with existing platforms
- H Not encountered any barriers at this stage
- Encountered in the deployment phase
- Encountered/expect to encounter this once deployed



What are the most important drivers for the deployment of IoT projects for your organisation?

Cost efficiencies	52%	Greater physical security	38%
Improve environmental sustainability	50%	Improve compliance/regulatory	37%
Increase staff productivity	47%	Greater automation	33%
Reduced downtime	47%	Improve customer experience	28%
Greater supply chain insight	46%	New revenue streams	27%
Better decision-making	39%	Lower insurance premiums	21%
Improve health and safety	39%	Other	4%

[1] https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/oil-and-gas-industry-outlook.html

At all stages of the oil and gas lifecycle there is a well understood concern regarding the impact of the process on the environment, with sustainability a board-level priority. The reputational and financial damages resulting from a public incident are a key driver for deployment throughout the oil and gas value chain, with regulators and environmental agencies issuing harsh penalties for transgressions. Just as importantly, oil and gas occupies a strategic position powering the world's economic engine and is therefore under increased threat of cyber-attacks. In early 2021 the Colonial Pipeline ransomware attack took out half of the US East Coast's fuel supply, causing consumer petrol prices to spike and demonstrating how vulnerable oil and gas infrastructure is to bad actors.

The Internet of Things (IoT) is helping businesses overcome challenges at all stages of the production cycle: from the efficient analysis of samples and unmanned exploration rigs, to wellhead and artificial lift monitoring, to pipeline monitoring and vehicle telemetry. The ability to monitor, manage and automate remotely is critical to the success of the sector where so much of the activity goes on in inhospitable conditions. In many ways oil and gas was an early adopter of IoT technology, particularly for monitoring extraction, and it has delivered successful outcomes for the sector. However; the world's increasing interconnectivity is changing how IoT technology needs to be implemented and the increasing number of connected nodes opens up the sector to more cyber-security challenges.

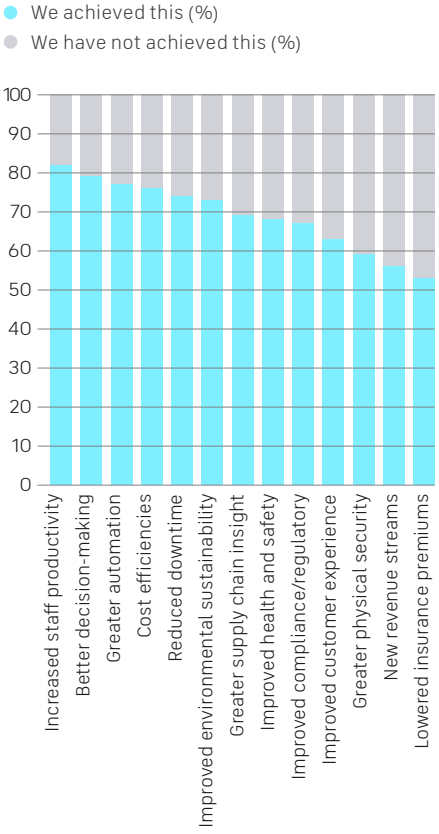
In order to respond to these challenges, a robust strategy is essential and our research found 49 per cent have a formal IoT strategy in place, which is the highest proportion of any of the sectors we surveyed. This rises as high as 56 per cent in North America and 65 per cent for those in the Middle East where some of the larger organisations we polled are based.

The oil and gas sector has been hit particularly hard by Covid-19, which is no surprise given the impact of global shutdowns on vehicle usage and aviation. In our survey, 42 per cent say the pandemic has negatively influenced their ability to operate; however those with an IoT strategy were less likely to say their business was negatively affected, thanks in part to IoT's ability to keep the value chain efficient. Oil and gas respondents were also slightly more likely to have accelerated deployment of IoT projects in response to the pandemic than the wider sample, demonstrating their faith in the technology to enable business continuity.

All in all, our research found the oil and gas sector to be at an inflexion point with a lot of change occurring to meet the challenges it faces. There has been a rapid increase in adoption over H2 2020 although further board prioritisation is needed to insure that it supports business operations optimally. The good news is investment beyond the resources of any other sector appears to be earmarked to support future growth and there are clear results and confidence in the technology to support oil and gas businesses.

From a connectivity and data standpoint the sector faces a number of challenges, though it demonstrates a level of maturity versus the sample, with the highest proportion of our respondents using backup connectivity to ensure continuous data collection and the highest number using real-time data collection. The sector is highly security aware and considered in the need to continue to improve its defences, though this varies by region. The Middle East and North America – two highly established regions for oil and gas production – are also more mature technologically than other regions we surveyed.

How would you score your organisation's achievement of expected benefits of IoT projects?



"49 per cent have a formal IoT strategy in place - the highest proportion of any sector we surveyed."

ADOPTION

Just under three-quarters of oil and gas respondents (74 per cent) have fully deployed at least one IoT project, with most of the remainder either currently trialling it or planning to do so in the next 12 months. 24 per cent have deployed at least one project in the last six months alone, demonstrating the importance oil and gas companies are attributing to the technology as a way to respond to industry challenges.

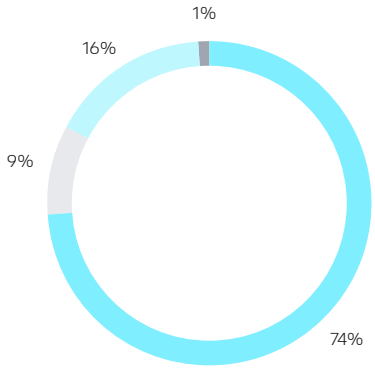
The drivers for deploying IoT projects further reflect the challenges faced by the sector. Cost efficiencies (52 per cent) was the top driver for adopting IoT, narrowly edging out improved environmental sustainability (50 per cent). That these two are the top drivers is entirely unsurprising given the board-level priorities of oil and gas companies. Better staff productivity was close behind on 47 per cent.

Perhaps reflecting the investments and relative maturity in the sector, the majority of organisations surveyed have achieved the benefits they set out to achieve with IoT projects. This was particularly the case for improved productivity (82 per cent), greater cost efficiencies (76 per cent), and better environmental sustainability (73 per cent). However, there are still certain areas that require more work to be done for oil and gas companies to achieve the expected benefits from IoT projects, such as using IoT to access new revenue streams (44 per cent not achieved) and improved physical security (42 per cent not achieved).

The most common use case, either fully deployed or in-trial, is pipeline monitoring (62 per cent) where IoT can be used to track flow rate, temperature and a variety of other metrics, as well as physical security. This was followed by vehicular tracking, asset tracking and route optimisation (58 per cent) and well-head monitoring (56 per cent). Additionally, 50 per cent of respondents have either already deployed or are trialling IoT projects in people tracking to enhance health and safety, with this representing the largest growth area in the next year with over a quarter (27 per cent) planning to fully deploy in that time.

While the sector is relatively advanced in its adoption of IoT, it also faces a number of barriers that are hampering optimum results and in some cases causing projects to fail before full deployment. A lack of in-house IoT skills and a lack of capital are the top reasons getting in the way of successful project deployment (both cited by 34 per cent of respondents). A lack of turnkey solutions is next (33 per cent), followed by security implications and consistent and reliable connectivity (both with 31 per cent).

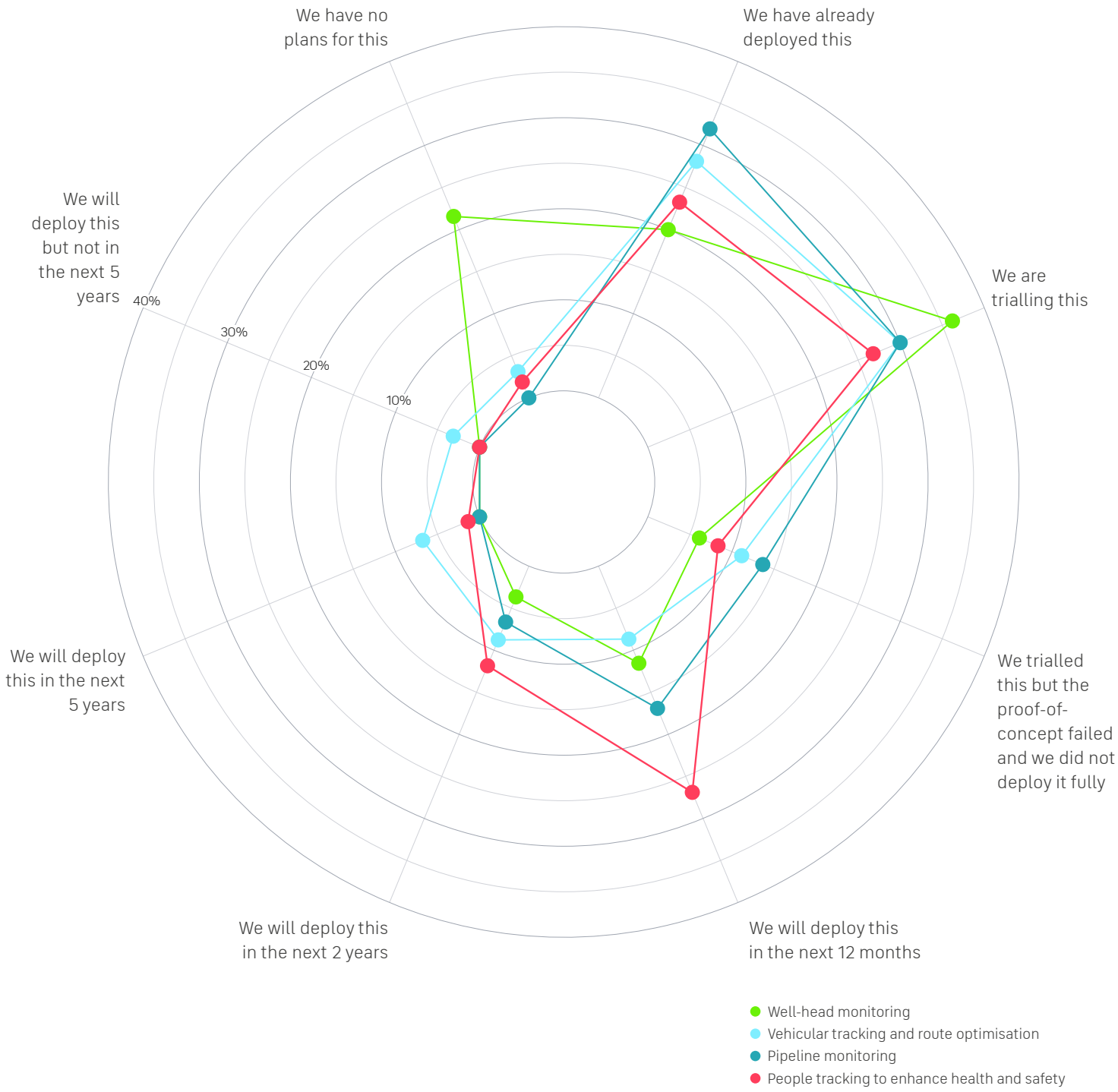
Once projects are deployed the biggest barriers to success were stated as integrating IoT technology with existing platforms (48 per cent), IoT not being prioritised by the board (40 per cent) and security implications (38 per cent). Some of the challenges regarding the integration of IoT technology with existing platforms is likely to relate to the older generation machine-to-machine (M2M) technologies that many oil and gas companies have used, but which need to be updated to reflect the increasingly interoperable networks that IoT is increasingly reliant on. A potential lack of board prioritisation of IoT will need to be addressed to ensure that IoT is well equipped to help overcome the challenges facing the sector.



What is your current status in terms of deploying IoT projects?

- Fully deployed
- Currently trialling
- Planning to trial within 12 months
- Planning to trial in 18 months – 2 years

What IoT projects has your organisation already deployed and what will your organisation deploy in the future?



CONNECTIVITY

The oil and gas industry needs to do more to put connectivity technologies to work according to the latest analysis by McKinsey. They argue 'advanced connectivity... could add up to $250 billion of value to the industry's upstream operations by 2030.'[2] Despite room for improvement in using connectivity to support IoT projects, there are some positive trends within the sector.

Satellite is the most widely used type of backhaul connectivity used in IoT projects (56 per cent), illustrating the demand for connectivity that works anywhere, in an industry where operations are remote and environments unforgiving. Predictably, it is more widely used by the exploration segment where certain types of satellite connectivity has inherent portability advantages. 80 per cent of respondents stated that satellite connectivity provides crucial support to their organisation's IoT communications networks. But to ensure, as ever, that businesses get the most from their satellite connectivity, the right form needs to be considered. For IoT dedicated use-cases frequencies like L-band are ideal, providing mobility, reliability.

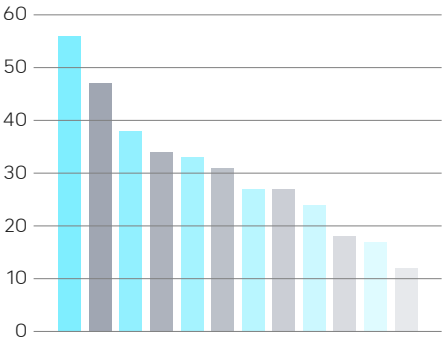
Private cellular connectivity was the next most popular long range connectivity type (34 per cent), only slightly more widely used than public cellular connectivity (33 per cent). Finally, fibre is also commonly used with 31 per cent of respondents indicating they use it for IoT projects. While terrestrial connectivity clearly has a role to play, 44 per cent of respondents say these connectivity types do not fulfil their needs in terms of helping them deploy IoT projects.

In terms of edge connectivity Wi-Fi figures most prominently with 47 per cent using it. While newer styles of Wi-Fi support more advanced features it may not be the best option for all edge use cases, particularly due to contention issues. Perhaps more appropriately, Long Range Wide Area Networks (LoRaWAN) and Bluetooth Low Energy (BLE) are also widely used by 27 per cent of respondents respectively.

66 per cent of respondents have experienced issues implementing IoT projects due to connectivity limitations, with 78 per cent stating they experienced problems during the trial and proof of concept phase. 61 per cent have seen disruption after deployment. To illustrate the importance of reliable connectivity 82 per cent agree that IoT projects have become much more successful since solving their connectivity challenges.

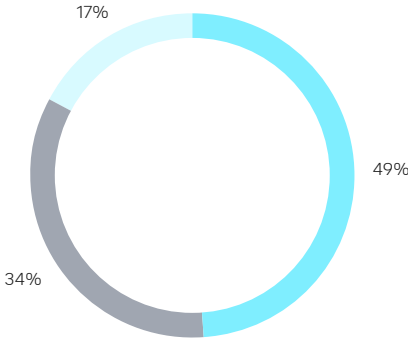
Mission critical data collection requires always on connectivity, with lost data potentially leading to outages bringing production to a halt and cost implications running into the millions of dollars. This is comparatively well understood within the oil and gas sector - compared to the others we surveyed - with 49 per cent of respondents indicating they use a backup connectivity type to keep data transfer going in the event of an outage. An additional 34 per cent continue collecting data offline, while 17 per cent will pause all data collection completely until the original connection is restored leading to lost data. 70 per cent of organisations in APAC use backup connections rather than offline data collection or pausing the process; this high proportion of respondents is also reflected in the largest companies (more than 5,000 employees).

When making a choice on connectivity type, oil and gas decision-makers take a number of attributes into consideration, of which security (49 per cent), network coverage (47 per cent) and reliability (46 per cent) are the top three. The prioritisation of secure connectivity underlines the increased risks that the sector faces, with only electrical utilities respondents rating this more of a necessity. All three attributes are however highly desirable in IoT connectivity and their choice again signals the maturity of the respondents in the sector.



What connectivity types does your organisation use in its IoT projects?

Satellite	56%
Wi-Fi	47%
Radio	38%
Cellular (private)	34%
Cellular (public)	33%
Fibre	31%
LoraWAN	27%
Bluetooth Low Energy (BLE)	27%
NB IoT	24%
Sigfox	18%
Zigbee	17%
Other	12%



In remote areas away from terrestrial communication, what do you do if unable to connect to your chosen connectivity type.

- Use a backup connection type to continue
- Continue collecting data offline until the connection is restored
- Pause all data collection until connection is restored

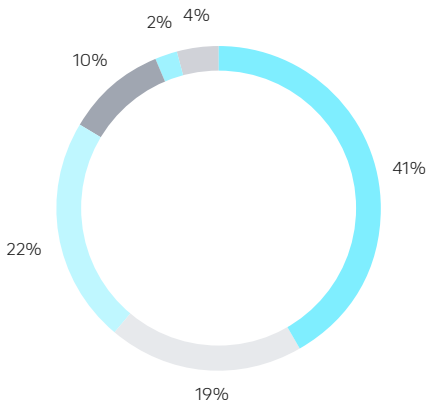
[2] https://www.mckinsey.com/industries/oil-and-gas/our-insights/how-tapping-connectivity-in-oil-and-gas-can-fuel-higher-performance

DATA

The all-important data produced in IoT projects needs to be in the right format, in the right hands, at the right time to be optimally turned into insight. Oil and gas professionals surveyed listed a variety of reasons why they struggle to leverage IoT data as effectively as possible. As is common across all sectors examined in this report, security is front of mind for many (53 per cent). This is followed by a lag between data collection and availability (52 per cent), a lack of IoT data strategy (34 per cent) and not having the skills to properly extract and use data (34 per cent). Security concerns are much more prominent for those working in exploration (69 per cent), and less so for those in distribution (38 per cent), with a similar trend seen with a lack of an IoT data strategy and data skills shortages.

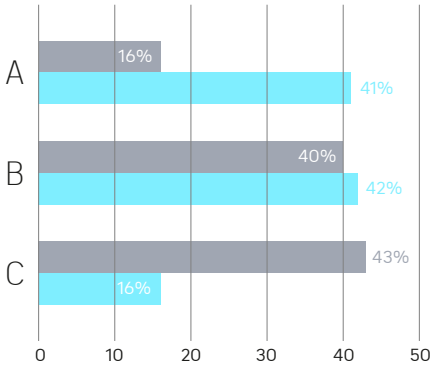
IoT strategies are important to govern the flow of data inside and outside an organisation. Privacy is evidently front of mind in the approaches to data sharing within the sector: oil and gas respondents contain the lowest proportion saying they share IoT data outside the organisation (16 per cent). 40 per cent of respondents stated they currently make IoT data available to anyone in the organisation, while 43 per cent limit access to a select number of departments within the business. Given the highly sensitive nature of some data and a lack of data strategy in some areas, this might be prudent but a rationalised sharing strategy will help optimise value chains in the future and help the sector achieve its goals. This point is understood amongst 41 per cent of respondents who indicate they will make data available to external parties in the future.

Analysing the intervals at which data is collected, oil and gas is ahead of the curve in terms of real-time collection (41 per cent, compared to a wider sample average of 30 per cent), with this interval well ahead of any other we examined. The Middle East and North America are even further ahead in this area, recording 70 per cent and 43 per cent respectively. The largest companies also demonstrate a similar commitment to real-time data collection, with 49 per cent of those with over 5,000 employees doing so. An important next step is for other regions and smaller organisations to catch up, as more frequent data collection makes it easier for organisations to optimise their operations and respond to shifts in demand.



At what intervals do you typically gather IoT data points?

- In real-time
- Within half an hour
- Hourly
- Every two hours
- Every four hours
- Daily



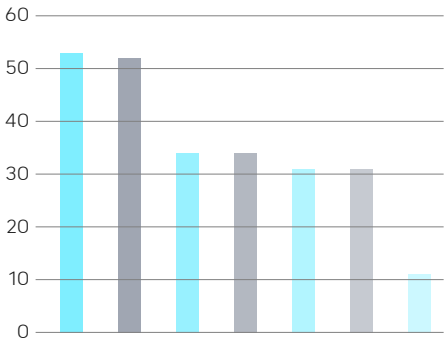
To what extent does/will your organisation share non-sensitive IoT data?

A It is available to anyone in the organisation, or our partners, to access and use

B It is available to anyone in our organisation to access and use

C It is only available to certain departments involved in the IoT project

Currently In the future

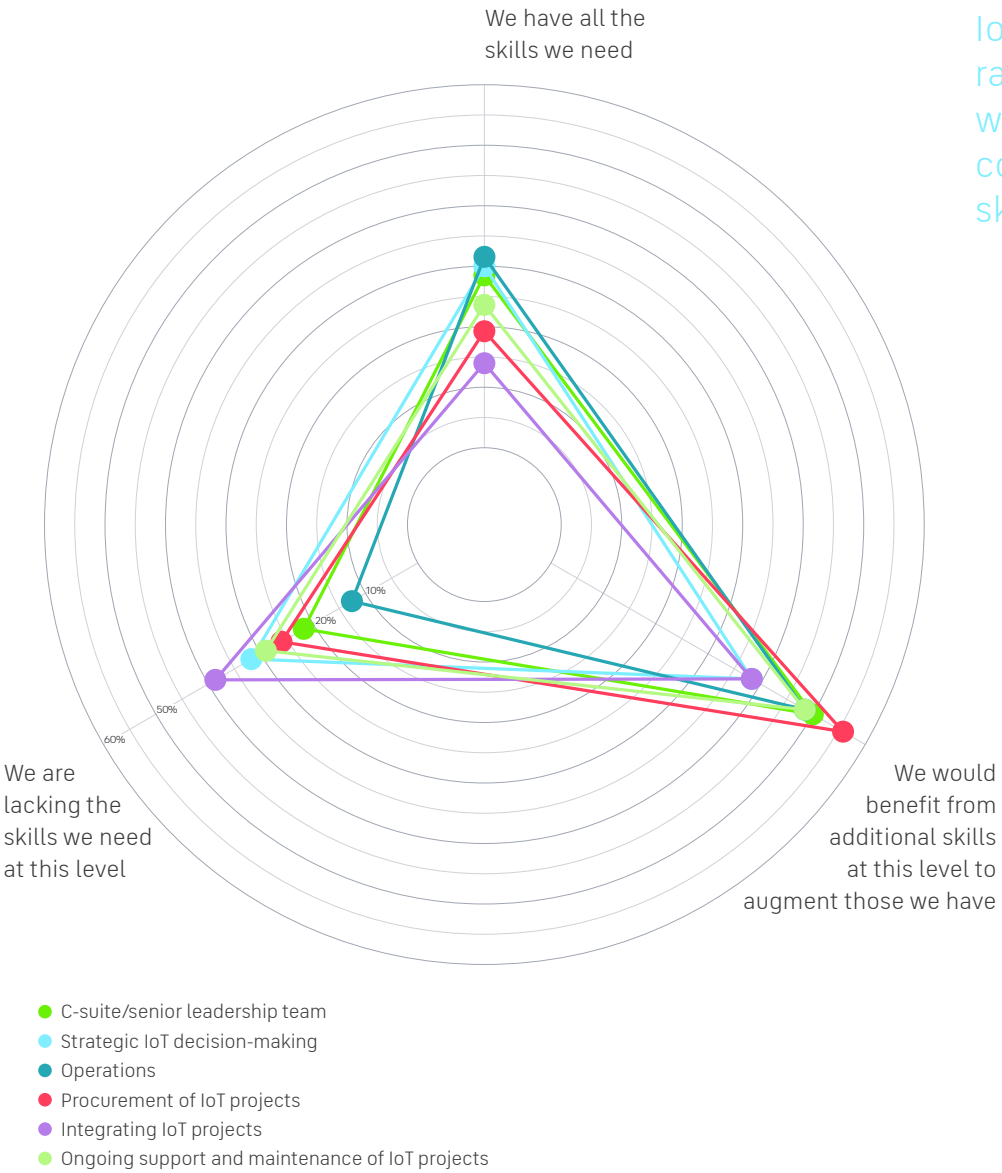


What barriers prevent your organisation from using data optimally?

Security/privacy concerns	53%
Lag between data collection and data being available	52%
Lack of IoT data strategy	34%
We don't have the skills to extract/use data	34%
Data is stored in an unusable format	31%
There is such a large volume of data we struggle to utilise it	31%
We are able to use data as effectively as possible	11%

SKILLS

Does your organisation have the skills needed to fulfil IoT projects at different levels?



"The additional skills that are needed to deliver IoT projects are wide-ranging in the sector, with a majority citing connectivity technology skills and security skills."

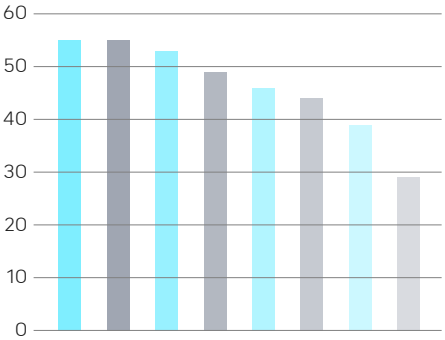
Earlier we outlined the biggest barrier impacting deployment was a lack of in-house skills, while the biggest barrier once the project was deployed was a lack of IoT prioritisation by the board. These challenges are again prominent as we look more closely at the skills required by organisations.

Our respondents stated that the area of the business they most lacked the skills in was around the integration of IoT projects (38 per cent), with only 14 per cent stating they have all the skills to do this effectively, again underlining some of the challenges faced around integrating newer connectivity methods with older systems. Close behind was strategic decision-making with 32 per cent indicating they are lacking the skills needed at this level, although conversely roughly a third (30 per cent) of the respondents actually stated they had all the skills they needed here. The lack of strategic decision making skills was most keenly felt in Russia and the Stans where only five per cent of respondents felt they had all the necessary skills.

The additional skills that are needed to deliver IoT projects are wide-ranging in the sector, with a majority citing connectivity technology skills and security skills (both 55 per cent). 53 per cent say better analytical and data science skills are required, 49 per cent need additional project management skills and 46 per cent want to see improved competencies in technical support. Respondents working in exploration are more likely to cite security skills as a requirement (63 per cent), while those in distribution are less likely to do so (46 per cent) cent). This hopefully suggests that they have already made steps to address potential vulnerabilities which would be as high, if not higher, with permanent pipeline infrastructure.

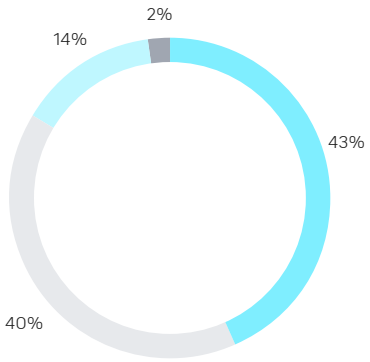
Purchasing decisions around IoT projects are most likely to be made by senior management, such as heads of departments (43 per cent), although C-suite executives (22 per cent) and middle management (24 per cent) are also involved.

Regarding off-the-shelf IoT solutions that meet the needs of oil and gas firms, there is a little more to be desired. Overall, 43 per cent are aware of solutions that can assist them in their IoT objectives, which is lower than the overall sample average of 50 per cent. A total of 54 per cent believe that external providers either only meet some of their needs or, worse, meet none of them at all. Finally, in terms of organisation size, mid-sized organisations tend to be more aware of off the shelf IoT solutions in the marketplace than smaller ones (58 per cent for companies with between 501 and 1,000 and 55 per cent for those with 1,001 to 3,000 employees). Overall, however, there is plenty for IoT providers to do to improve their offerings and build better connections with oil and gas companies.



What additional skills do you need to deliver IoT projects?

Connectivity technology skills	55%
Security skills	55%
Analytical/ data science skills	53%
Project management skills	49%
Technical support skills	46%
Strategic skills	44%
Procurement skills	39%
Database management skills	29%



Are you aware of off-the-shelf IoT solutions that meet your needs?

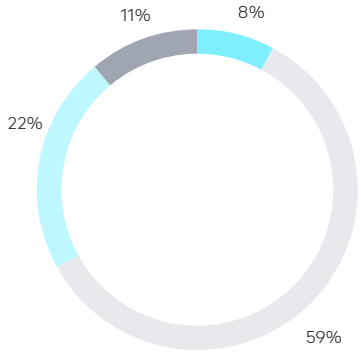
- Yes, we are aware
- No, providers only meet some of our needs
- No, providers don't meet our needs at all
- Don't know

SECURITY

Security has cropped up consistently throughout this report as a major concern for oil and gas respondents, so examining exactly what these issues are will help the sector take remedial steps. Poor network security and the risk of external cyber-attacks are the two biggest fears, cited by a majority of 58 per cent and 54 per cent, respectively. Those working in exploration are particularly concerned about poor network security, with 72 per cent of respondents within the sub-sector citing this as one of the biggest challenges associated with the use of IoT projects within their organisation. Other key security challenges across the sector include insecure storage of collected data (48 per cent) and insecure or unencrypted edge networks (43 per cent).

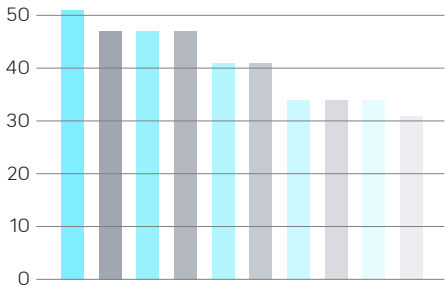
Overall, 92 per cent of oil and gas respondents believe their IoT defences could be more robust, with 11 per cent hoping to see a major overhaul. Perhaps driven by an informed security - conscious mindset, only 8 per cent of respondents stated that their organisations' IoT solutions have robust cyber-security defences from end-to-end in compliance with the relevant ISO standard. This was significantly lower than in other sectors we surveyed but may well be an indication of an increased understanding of the potential risks. Respondents from Russia and the Stans were most likely to indicate their cyber-security defences have not been a priority and could be vastly improved, which suggests a major problem that needs to be resolved for companies within the region.

The positive news is that the sector is heavily engaged in efforts to improve the situation. Popular measures include creation of an internal IoT security policy (51 per cent), upgrades to existing security technology, investing in new security solutions and training employees to better understand IoT (all 47 per cent). Those working in exploration – the sub-sector most concerned about digital security – are generally more engaged than those in extraction or distribution in building better defences. Two-thirds (66 per cent) of exploration respondents have already created an internal IoT security policy and 63 per cent invested in new security technologies, which shows their priorities are in the right place. In terms of accessing the requisite security skills Russia, the Stans and the Middle-East are more likely to look for support from a third party rather than bringing those skills in house as with the rest of the World.



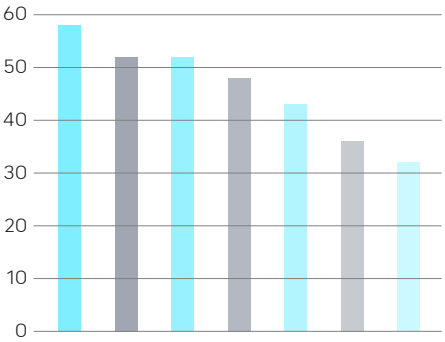
Which of the following statements are accurate regarding the security of your IoT projects?

- We have robust cyber-defences
- Our defences are good but could be stronger
- We need much better cyber-defences
- Our cyber-defences need to be vastly improved



What changes have you made to address IoT security concerns?

Creation of an internal IoT security policy	51%
Investing in new security technologies	47%
Training employees on IoT	47%
Upgrading existing security technologies	47%
Creation of an external IoT security policy for suppliers and partners	41%
Communicating to customers on the use of IoT	41%
Partnering with a third party	34%
Hiring skilled staff	34%
Securing physical assets such as sensor nodes	34%
Implementing a backup connectivity network	31%



What are your biggest IoT security challenges?

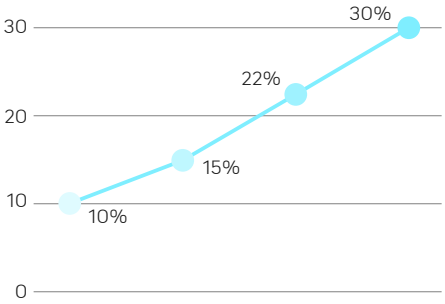
Poor network security	58%
Risk of external cyber-attack	52%
Potential mishandling/misuse of data by employees	52%
Insecure storage of data collected	48%
Insecure/unencrypted edge networks	43%
Supplier/partner data regulation compliance requirements	36%
Internal data regulation and compliance requirements	32%

INVESTMENT

The average investment in IoT projects per organisation in the oil and gas sector is estimated to be $3,247, 753 over the next three years, which represents the highest average of any sector we surveyed. A further 11 per cent of respondents are expecting to spend in excess of $5,000,000, also the highest largest number amongst our respondents. As would be expected, the smaller organisations have a lower planned spend than the average, while the biggest companies expect to commit the most (an average of $7,100,000 for those with more than 5,000 employees). Given the huge global appetite for oil and gas products, these large budgets come as no surprise.

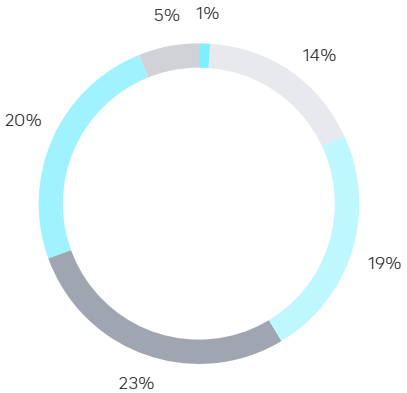
Like the other sectors we surveyed, it is clear that IoT has taken centre stage as a lever for optimisation. Respondents indicated they will dedicate more budget to IoT projects than others such as big data analytics, cloud computing or next generation security over the next three years. This trend is particularly evident in the Middle East where 13.6 per cent of budgets will be spent on IoT in the next three years, while conversely, companies based in Russia and the Stans will only spend 5.3 per cent on IoT, preferring to invest in cloud computing and big data.

Complementing the sector's willingness to invest is a keen awareness of how IoT engagement can save the business money in both the short and long term. Currently, the average estimated saving for the business is 10 per cent, with this expected to rise to 15 per cent in 12 months. These short-term benefits are strong in themselves, but it is after three and five years where respondents feel they will truly reap the rewards, estimating an eventual cost saving of 30 per cent. Larger oil and gas organisations (more than 5,000 employees) expect to see even greater savings in the long term, expecting an average of 32 per cent in five years. Companies are clearly confident in IoT's ability to improve their business, but the next steps will be to make sure these aims are achieved in practice.



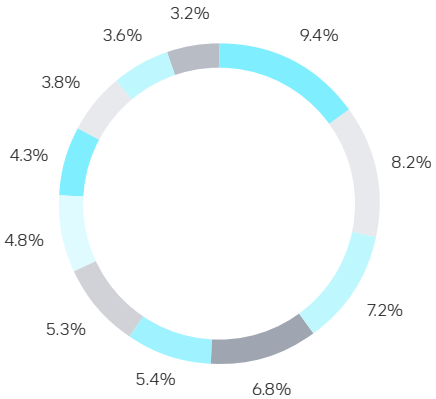
What proportion of your organisation's costs are saved/going to be saved from IoT projects?

Currently	10%
In 12 months	15%
In 3 years	22%
In 5 years	30%



What is your planned investment in IoT projects in the next three years?

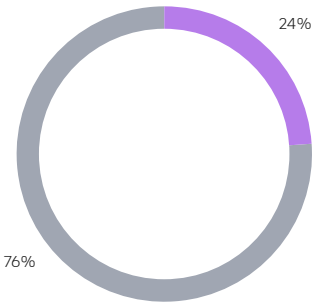
- $100,000 to $500,000
- $500,000 to $1,000,000
- $1,000,000 to $2,000,000
- $2,000,000 to $3,000,000
- $3,000,000 to $4,000,000
- $4,000,000 and above



What proportion of your IT budget will you spend on IoT projects in the next three years?

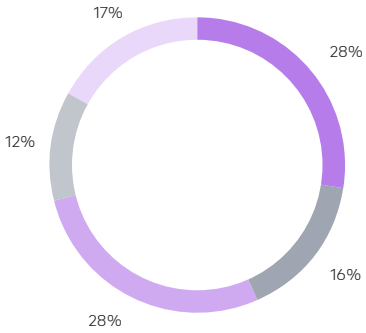
- IoT projects
- Cloud computing
- Big data analytics
- Next generation security
- Robotics
- Augmented Reality
- Machine Learning
- Virtual Reality
- Cognitive AI
- Blockchain
- 3D Printing

TRANSPORT AND LOGISTICS



Respondents by sub-sector (%)

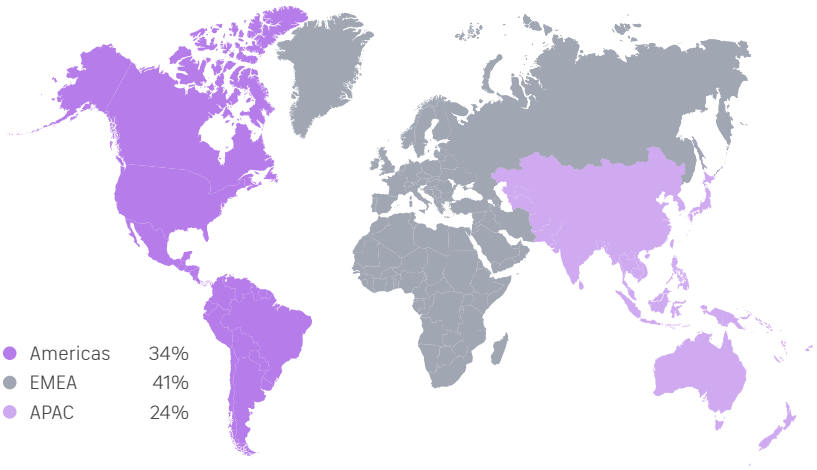
- Freight railway operators
- Logistics



Respondents by size of organisation (%)

- 251-500 employees
- 501–1,000 employees
- 1,001–3,000 employees
- 3,001–5,000 employees
- More than 5,000 employees

Respondents by region (%)



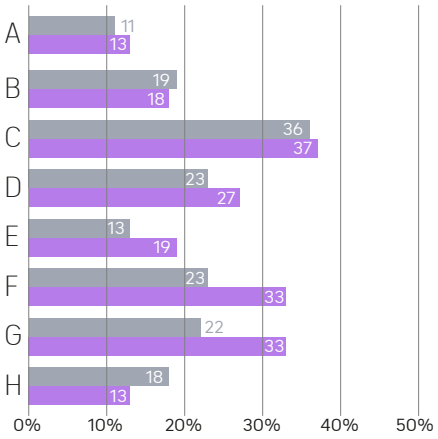
Americas	34%
EMEA	41%
APAC	24%

The increasing social mobility of urbanising populations and the correlated growth in demand for goods and services by both consumers and businesses worldwide is placing unprecedented demand on logistics networks. In addition, the transport and logistics industry also needs to meet increasingly stringent environmental and sustainability regulations, to minimise its impact on climate change. To ensure that global supply chains can meet the increasing demand for both people and things in the most efficient and sustainable ways possible, the industry is embracing digitalisation and accelerating its adoption of Internet of Things (IoT) technologies.

This acceleration in IoT adoption by transport and logistics companies has only increased over the course of the Covid-19 pandemic in the past 18 months. Over half (54 per cent) of all respondents from the sector noted that the many challenges related to Covid-19 have underlined the importance of IoT and automation to business success. 49 per cent of respondents having already accelerated deployments of their IoT projects in response to the challenges of the pandemic, with 41 per cent intending to start accelerating their adoption of IoT technologies within the next few years.

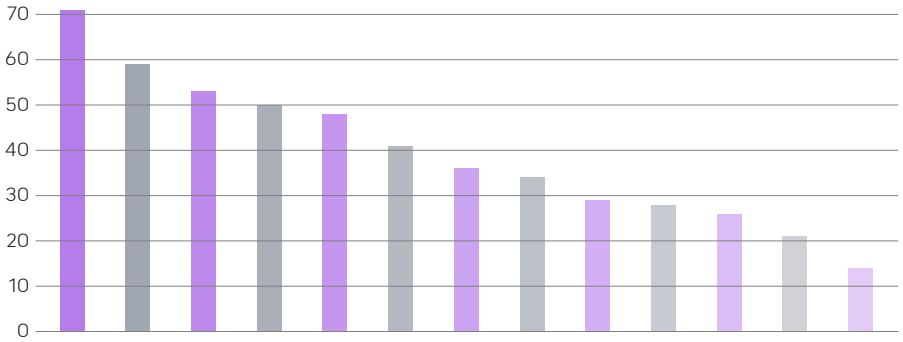
These findings reflect the increasingly pressurised state that global supply chains have been under since the start of the pandemic, with vaccine distribution logistics of utmost importance, grocery distribution challenged by restrictions in movement, and a greater demand for last-mile deliveries from home consumers. Despite the challenges to the transport and logistics industry caused by the Covid-19 pandemic, the encouraging findings from our research clearly reveal that the sector is taking all these challenges seriously, adopting IoT and other technologies to ensure tomorrow's land logistics networks are safer, more sustainable, and more efficient than ever before.

"Over half (54 per cent) of all logistics respondents in our research noted that the many challenges related to Covid-19 have underlined the importance of IoT."



What barriers, if any, does your organisation face in the deployment of IoT projects?

- A Lack of consistent and reliable connectivity
- B Lack of available capital to invest in IoT projects
- C A lack of in-house skills
- D Lack of turnkey/off-the-shelf solutions
- E IoT not being prioritised by the board
- F Security implications
- G Integrating IoT technology with existing platforms
- H Not encountered any barriers at this stage
- Encountered in the deployment phase
- Encountered/expect to encounter this once deployed



What are the most important drivers for the deployment of IoT projects for your organisation?

Greater supply chain insight	71%	Improve health and safety	34%
Cost efficiencies	59%	Reduced downtime	29%
Greater automation	53%	New revenue streams	28%
Better decision-making	50%	Improve compliance/regulatory	26%
Increase staff productivity	48%	Greater physical security	21%
Improve environmental sustainability	41%	Lower insurance premiums	14%
Improve customer experience	36%		

IoT is playing a key role in preparing transport and logistics businesses for the future, right across the value chain, from increasingly automated rail networks and signalling systems in the rail industry, through to highly accurate, real-time shipment and vehicle or goods tracking in logistics. Fundamentally, IoT is providing businesses with clear visibility and new, highly efficient forms of automation across the supply chain.

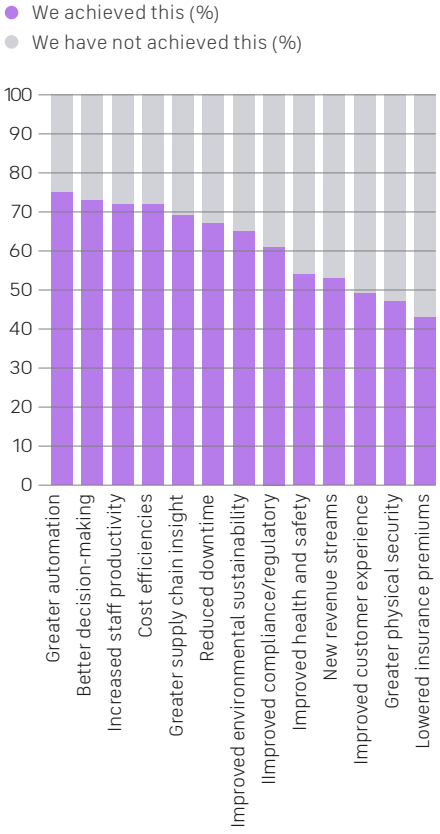
The rail sub-sector is leading the IoT charge in the transport and logistics industry, with 59 per cent of our rail respondents stating that they already have a formal IoT strategy in place, with every rail organisation polled having already fully deployed at least one IoT project within the last two years. The logistics sub-sector, while still demonstrating a high level of IoT maturity, is lagging slightly behind rail, with only 41 per cent of those businesses having a formal technology strategy and 63 per cent having already fully deployed projects. Additionally, there are regional variations in levels of IoT maturity: while 63 per cent of North American transport and logistics businesses have a formal IoT strategy, this drops to only 13 per cent of Latin American businesses.

Establishing a formal IoT strategy is essential, as it enables transport and logistics businesses to understand what areas of the business they need to extract data and insight from, as well as how they might automate operations. While most organisations in our research demonstrate a high level of IoT maturity, it is those businesses in APAC and North America, alongside the largest organisations of over 3,000 employees, that are farthest ahead in their journey. These trailblazers are not only investing the most, and expecting the highest returns, they are demonstrating how the industry can best utilise IoT.

Despite considerable progress being made across the sector over the last few years, there are several challenges stopping the transport and logistics industry from getting the optimal benefits from its IoT investments. The skills gap remains the biggest barrier to successful IoT adoption, with security, data analysis and connectivity skills in high demand. In terms of connectivity, more redundancy is needed to ensure consistent data collection, with only 28 per cent of all respondents using a backup connection type, preferring instead to either collect data offline or pause data collection until connections are restored. With greater automation and better decision making being key drivers for deployment of IoT we may see this trend shift in the coming years.

In addition to developing an improved connectivity backbone, which is needed to make IoT projects a true success, the transport and logistics sector also needs to focus more of its efforts and resources on developing better data strategies. This will encourage a more collaborative approach to enable the sharing of non-sensitive IoT data across and between businesses and their IoT technology partners. Encouragingly, from a security perspective, respondents indicated they have robust end-to-end cyber-security at a higher proportion than any other sector we surveyed. Finally, investment in IoT is slightly above the average, while experienced and expected ROI is slightly below the average.

How would you score your organisation's achievement of expected benefits of IoT projects?



ADOPTION

Just under three-quarters of our respondents in the transport and logistics sector (72 per cent) have fully deployed at least one IoT project, up from a different sample set with 40 percent in 2018. 29 per cent of companies have deployed fully within the last 12 months, demonstrating the fast maturing attitudes toward IoT in the sector. The remaining 28 per cent of respondents either plan to deploy the technology within the next two years or are currently trialling IoT projects.

As is the case with all the industries we surveyed in our research, the transport and logistics sector has faced numerous challenges related to Covid-19, with the rail industry being particularly hard hit. Over a third (36 per cent) of respondents from rail companies noted that the pandemic had negatively influenced their ability to operate , compared with 30 per cent for the overall transport and logistics sample. However, 54 per cent of all transport and logistics respondents also say that challenges related to the pandemic have underlined the importance of IoT and automation to business success. This will largely be a consequence of IoT data having an important role helping support organisational efficiencies in pressured supply chains. 90 per cent of our respondents also told us they have either accelerated deployment of IoT projects in response to the crisis or have plans to do so in the next two years.

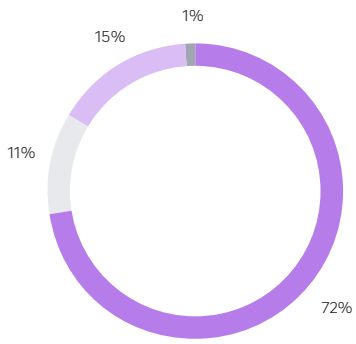
The drivers that are motivating the sector to deploy IoT projects further reflect the challenges facing the industry. Unsurprisingly greater supply chain insight is cited as the most important driver, with 71 per cent of respondents indicating they have adopted IoT for this reason. Not far behind is cost efficiencies (59 per cent), followed by greater automation (53 per cent) and better decision making (50 per cent). While greater insight over the supply chain is the most important driver for most regions, increased staff productivity was viewed as the most important driver of IoT usage in North America (81 per cent). Respondents in North America also listed the highest numbers of different drivers for using IoT, indicating a sophisticated understanding of the potential for IoT to increase competitive advantage.

In terms of use cases, the most common area IoT is being engaged in for rail respondents is automated rail signalling, where 55 per cent of all rail respondents have already deployed and an additional 32 per cent are in the trial phase. Wagon and cargo monitoring was in second place in the rail industry, with 41 per cent of respondents having actively deployed it. Elsewhere, in the logistics sub-sector, shipment and supply chain tracking was the most common area in which IoT projects are in use, with 37 per cent of logistics respondents having already deployed these, and 21 per cent currently trialling them.

Over the next few years, the industry is set to see an increasing number of fully deployed IoT projects focused on vehicular and asset tracking and route optimisation, with 27 per cent of all respondents currently trialling these. Other popular IoT projects currently being trialled include trackside environment monitoring, for events such as flooding and rock slides (32 per cent of rail respondents) and, potentially supporting the need to ship Covid-19 vaccines safely and securely, cold chain tracking (26 per cent of logistics respondents). As you would expect, it is the larger organisations (over 5,000 employees) that have already successfully deployed the greatest number of IoT projects. 88 per cent of those respondents have already leveraged IoT for shipment and supply chain tracking, and 60 per cent for vehicular tracking and route optimisation.

The most likely transport and logistics IoT use case to fail in the trial stage leading to it not being deployed was vehicular and asset tracking and route optimisation. 10 per cent of all respondents indicated a failed proof-of-concept, which may be caused by a lack of in-house skills (36 per cent). Other barriers at the deployment phase were security implications (23 per cent) and lack of turnkey solutions (23 per cent). Once projects were deployed respondents indicated the biggest barriers continued to be a lack of in-house skills (37 per cent), security implications and integrating IoT technology with existing platforms (both 33 per cent).

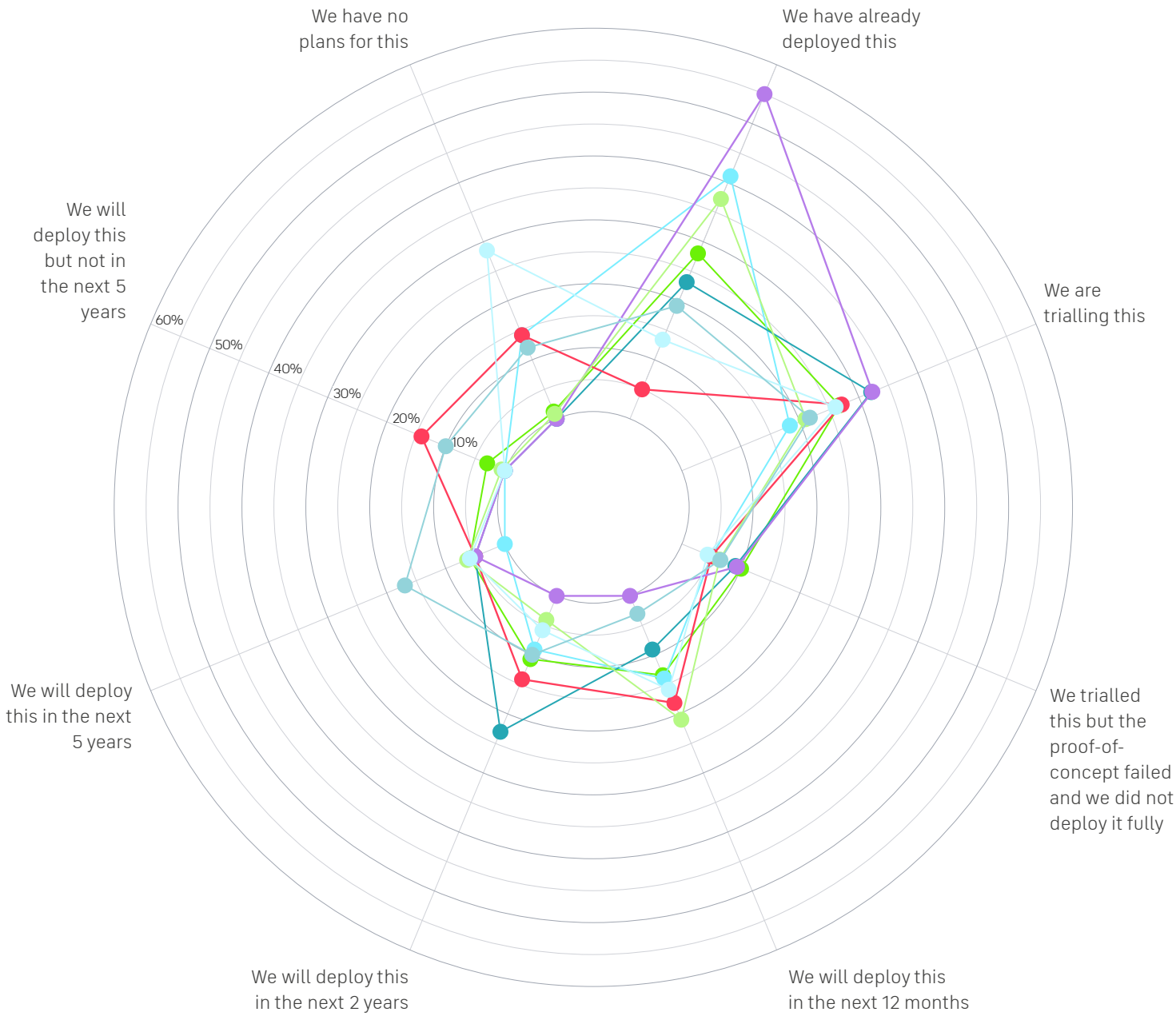
Encouragingly, most organisations surveyed have already realised many of the benefits they set out to achieve with IoT projects. This was particularly the case for greater automation (75 per cent), better decision making (73 per cent), increased staff productivity and cost efficiencies (both 72 per cent) and greater supply chain insight (69 per cent). However, there remain areas where desired benefits have not yet been achieved. Such as lowered insurance premiums (54 per cent not achieved), greater physical security (53 per cent not achieved) and improved customer experience (51 per cent not achieved). Given the recent uptick in last-mile logistics to home consumers during the pandemic, using IoT to improve the customer experience will need to be looked at to drive differentiation in a crowded market-place.



What is your current status in terms of deploying IoT projects?

- Fully deployed
- Currently trialling
- Planning to trial within 12 months
- Planning to trial in 18 months – 2 years

What IoT projects has your organisation already deployed and what will your organisation deploy in the future?



Note: some use cases specific to sub-sector - percentage of sub-sector shown.

- Vehicular and asset tracking and route optimisation (rail and logistics)
- Wagon and cargo monitoring (rail)
- Trackside environment monitoring (rail)
- Natural disaster monitoring (rail)
- Automated rail signalling (rail)
- Shipment/ supply chain tracking (logistics)
- Cold chain tracking (logistics)
- People tracking to enhance health and safety (rail and logistics)

CONNECTIVITY

Establishing the optimal mix of connectivity technologies is essential for transport and logistics businesses to realise the numerous benefits that IoT can deliver. And while our research reveals several positive trends within the industry, there is still plenty of room for improvement in using the right connectivity to support IoT projects. 54 per cent of all respondents agreed that their organisation has struggled to deploy IoT due to connectivity issues in areas they want to deploy it, and 59 per cent saw connectivity challenges in the trial phase.

Our transport and logistics respondents employ a wide range of connectivity types in their IoT projects, combining both short- and long-range technologies with three types used on average – common to our average across all sectors. With one notable exception: Latin American businesses are lagging when it comes to the average number of connectivity types in use, with an average of only two types used.

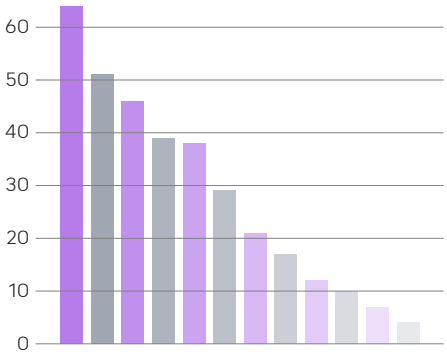
Overall, only 24 per cent of transport and logistics organisations consider public terrestrial networks (such as cellular or fibre) to be completely suitable for IoT connectivity. And the majority (59 per cent) agree that satellite connectivity provides crucial support to their organisation's IoT comms networks. That said, there is still a very high reliance on public cellular networks across the sector, with 46 per cent using public cellular infrastructure as a long-range IoT connectivity solution. This compares to only 38 per cent of respondents using satellite in their IoT projects, considerably lower than the 47 per cent average across all industries surveyed. This is an interesting finding given the potential advantages satellite optimised for mobility purposes can provide to moving assets, particularly as a backup connectivity type.

In terms of edge connectivity, Wi-Fi is by far the most popular short-range connectivity type (64 per cent), followed by Bluetooth Low Energy (BLE) with 39 per cent. The fact that BLE should rank much higher in usage than other sectors is not surprising given its established role in tracking consignments in the logistics sector. The sector also lags, noticeably, behind all other industry sectors in our research in its usage of LPWAN technologies such as LoRaWAN (17 per cent) and Sigfox (12 per cent).

Following the trial or proof of concept phase, connectivity issues continue to cause disruption for 58 per cent of all transport and logistics respondents even after IoT projects have been fully deployed. This poses questions about the suitability of the connectivity mix many transport and logistics businesses are using in their IoT projects. 78 per cent agree that their IoT projects have enjoyed much more success since solving their connectivity challenges.

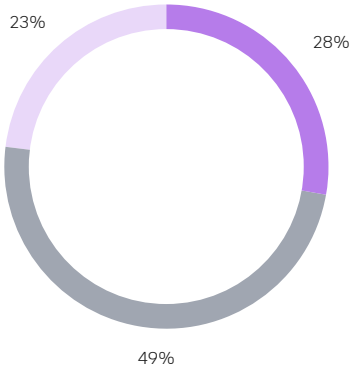
When choosing a connectivity type, logistics respondents indicated a range of preferences in the qualities they wanted, with reliability the most cited (47 per cent), followed by network coverage (44 per cent), security (41 per cent), bandwidth/speed (36 per cent) and cost (33 per cent).

That the sector has the lowest number of respondents from across all industries that use a backup connectivity method to avoid losing data in remote areas away from terrestrial comms (28 per cent), is surprising. Instead, 49 per cent indicated that their operations would go offline, and 23 per cent will pause all data collection completely until the original connection is restored. Of course, this may well be because much transport and logistics infrastructure is focused in and around urban areas, unlike some of the other industry sectors in this report. However, a single connectivity outage anywhere across the supply chain can cause costly disruption elsewhere, from shipping freight globally through to ensuring a last-mile consumer delivery reaches its destination safely and on time.



What connectivity types does your organisation use in its IoT projects?

Wi-Fi	64%
Radio	51%
Cellular (public)	46%
Bluetooth Low Energy (BLE)	39%
Satellite	38%
Fibre	29%
Cellular (private)	21%
LoraWAN	17%
Sigfox	12%
NB IoT	10%
Zigbee	7%
Other	4%



In remote areas away from terrestrial communication, what do you do if unable to connect to your chosen connectivity type?

- Use a backup connection type to continue
- Continue collecting data offline until the connection is restored
- Pause all data collection until connection is restored

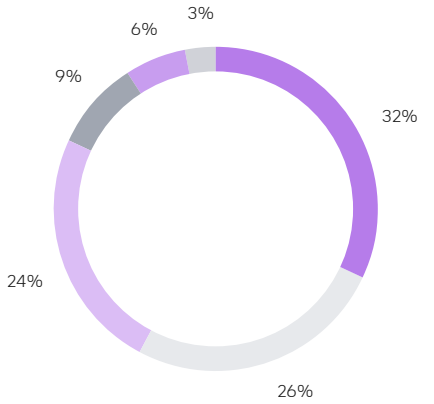
DATA

To extract the maximum value from the data gathered by their IoT projects, transport and logistics businesses need to ensure that this data is shared with the right people, at the right time and in the right format. There are a few reasons why rail and logistics companies are prevented from using the IoT data they collect as effectively as possible, with security and privacy concerns by far the most prevalent at 59 per cent. This is followed by a lag between data collection and availability (41 per cent), a lack of an IoT data strategy (27 per cent) and not having the relevant skills to properly extract and use data (23 per cent).

In the rail industry, for example, where operators are increasingly using autonomous train and signalling control technologies in some of the world's most remote regions, it is essential, for reasons of safety and efficiency, that the data generated by IoT sensors is made available securely, in real-time and is instantly available to rail network managers or controllers. For these reasons, the rail industry is certainly ahead of the curve as far as data sharing is concerned, with 36 per cent of rail respondents making data available to anyone in their organisations, or their partners, to access and use. This is compared to an average of only 20 per cent of respondents across all industry sectors in our research.

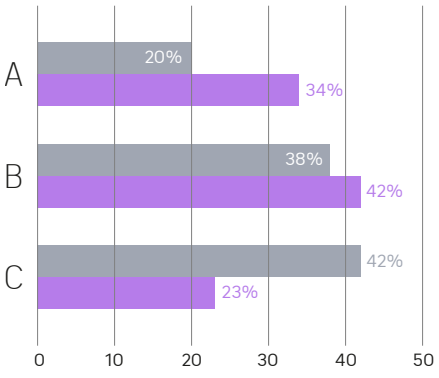
The logistics sector tells a slightly different story with only 15 per cent currently sharing their data across partners and their organisation. However; this is set to improve in the future with this figure increasing to 31 per cent, a change that will positively enhance the sector's ability to improve supply chain efficiency.

Finally, as mentioned above, the importance of receiving IoT data in a timely manner is crucial to ensure safe and efficient business critical operations across rail networks or logistics supply chains. That's why, in terms of the frequency that data is collected in transport and logistics projects, the sector is slightly ahead of some of the others that we investigated, with 32 per cent using real-time data collection. This focus on real-time data collection rises to 41 per cent of rail businesses and to 73 per cent for the largest transport and logistics organisations (over 5,000 employees) that are leading the way in the adoption of progressive practices.



At what intervals do you typically gather IoT data points?

- In real-time
- Within half an hour
- Hourly
- Every two hours
- Every four hours
- Daily



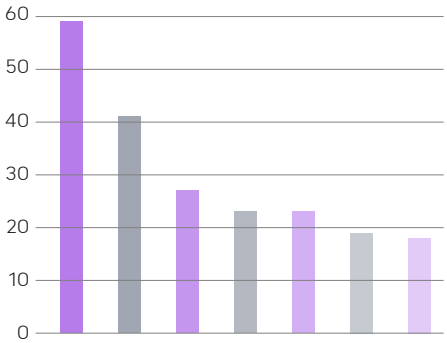
To what extent does/will your organisation share non-sensitive IoT data?

A It is available to anyone in the organisation, or our partners, to access and use

B It is available to anyone in our organisation to access and use

C It is only available to certain departments involved in the IoT project

Currently In the future

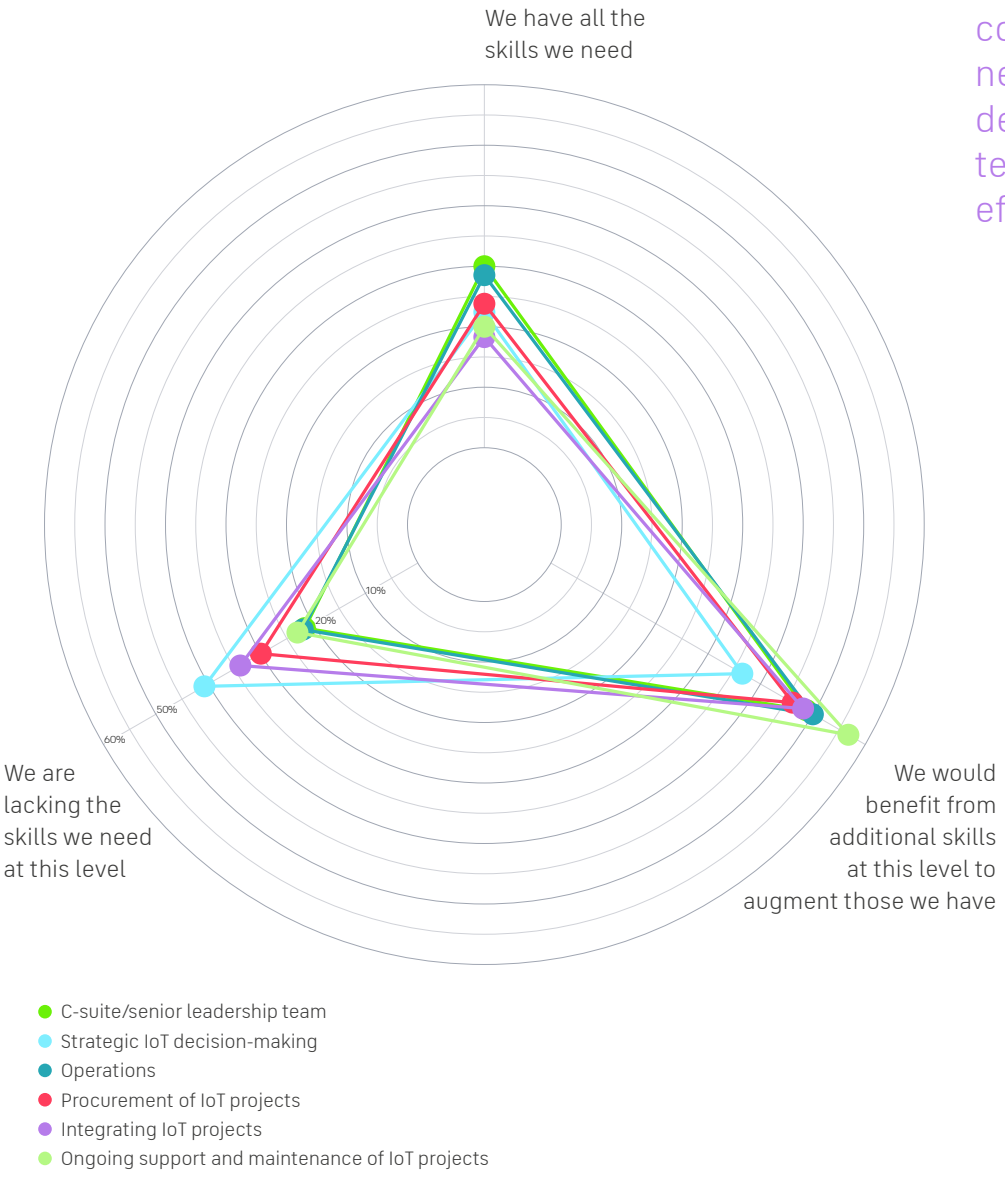


What barriers prevent your organisation from using data optimally?

Security/privacy concerns	59%
Lag between data collection and data being available	41%
Lack of IoT data strategy	27%
There is such a large volume of data we struggle to utilise it	23%
We don't have the skills to extract/use data	23%
Data is stored in an unusable format	19%
We are able to use data as effectively as possible	18%

SKILLS

Does your organisation have the skills needed to fulfil IoT projects at different levels?



"Both rail and logistics companies need to consider the skillsets needed to successfully deliver the benefits of the technology, and make efforts to upskill."

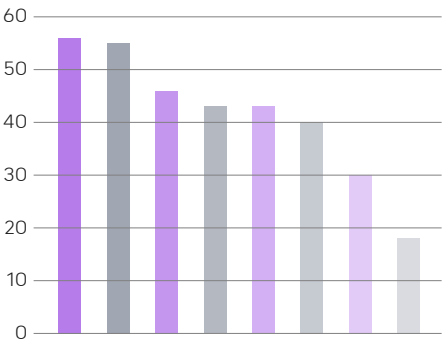
From the trial phase through to the post-deployment phase of IoT projects across the transport and logistics sector, the skills gap remains the biggest barrier to successful IoT adoption. Both rail and logistics companies need to consider the skillsets needed to successfully deliver the benefits of the technology, and make efforts to upskill, hire or work with relevant service providers to fill the gaps.

Transport and logistics respondents stated that area of the business they most lacked the skills in was strategic IoT decision-making (41 per cent), with only 22 per cent stating they have all the skills to do this effectively. The most skilled personnel were found at C-suite level (30 per cent), with the least number of sufficiently skilled workers at the integration level (18 per cent). This skills differential is even more pronounced for rail companies, with 36 per cent having all the skills they need at C-suite level, yet only 9 per cent at integration level. And for the largest organisations surveyed (over 5,000 employees), who cite 60 per cent at C-suite level, and only 7 per cent at integration level.

To address deficiencies, security skills are most sought after (cited by 56 per cent), followed by technical support skills (55 per cent), analytical/data science skills (46 per cent) and connectivity technology skills (43 per cent). Respondents from Latin America are severely lacking security skills (87 per cent) and far more likely to indicate they were lacking skills of all kinds than the rest of the sample set we interviewed. While a much higher proportion of smaller organisations (251 to 500 employees) lack the procurement skills they need to make sure they bring onboard the solutions they need to deliver their IoT projects.

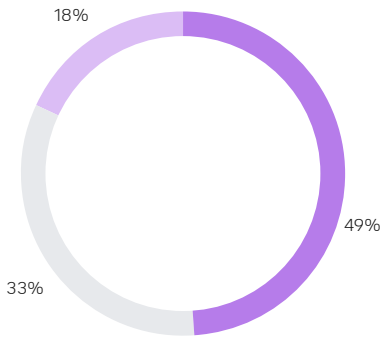
Purchasing decisions around IoT projects are most likely to be made by senior management in logistics companies (46 per cent) while rail companies are most likely to have middle managers in departments making the decisions (45 per cent). Smaller transport and logistics businesses are more likely to have C-suite and senior management involvement in IoT purchasing decisions, and larger organisations more likely to have IoT buying power at middle management level.

Finally, just under half of all transport and logistics respondents polled (49 per cent) are aware of off-the-shelf IoT solutions that can help them meet their organisation's needs, with the rail industry demonstrating a slightly higher awareness (59 per cent) when compared to the logistics industry (46 per cent). And, as would be expected, this figure rises with the size of the organisation, from 32 per cent for smaller organisations (251 to 500 employees) up to 67 per cent for companies with over 5,000 employees. Nearly a quarter (22 per cent) of logistics companies state that off-the-shelf IoT solutions don't meet their needs. All of which confirms that IoT service providers still have a considerable amount of work to do to build strategic relationships and tailor their offerings to meet the needs of these businesses.



What additional skills do you need to deliver IoT projects?

Security skills	56%
Technical support skills	55%
Analytical/ data science skills	46%
Project management skills	43%
Connectivity technology skills	43%
Strategic skills	40%
Procurement skills	30%
Database management skills	18%



Are you aware of off-the-shelf IoT solutions that meet your needs?

- Yes, we are aware
- No, providers only meet some of our needs
- No, providers don't meet our needs at all

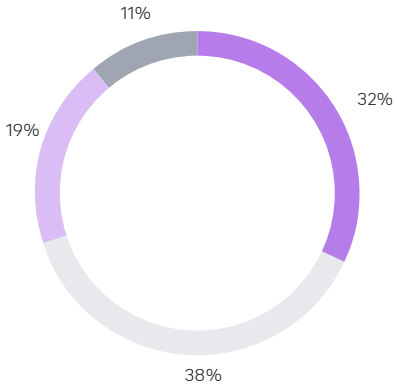
SECURITY

The increasing use of connected assets in IoT deployments across multi-modal supply chains in the transport and logistics industry only serves to increase the vulnerability of rail and logistics companies to cyber-security threats. As the entire transport and logistics industry across road, sea, air, and rail becomes increasingly digitalised, more potential vulnerabilities appear, and the potential for cyber-criminals, hackers or hostile state actors to severely disrupt networks or obtain valuable commercial data increases.

Transport and logistics businesses are having to become equally smart in their approach to IoT security and data management strategies to combat these threats. Transport and logistics respondents listed insecure storage of data collected (48 per cent), insecure or unencrypted edge networks (47 per cent), potential misuse of data by employees or the risk of an external cyber-attack (both 44 per cent), as the primary security challenges associated with the use of IoT projects in their organisations. Rail operators are highly concerned about the risk of an external cyber-attack, with 55 per cent of respondents in the sub-sector citing this as their primary security challenge.

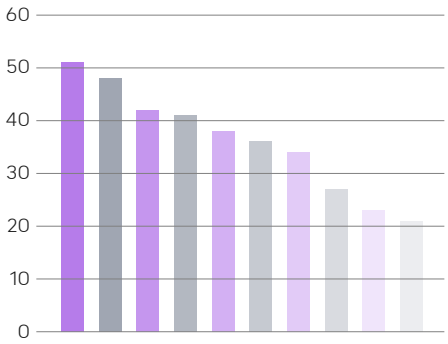
32 per cent of the respondents from the transport and logistics sample stated they had robust cyber-security defence from end-to-end in compliance with the relevant ISO standard, more than any other sector. Conversely a total of 68 per cent believe that their organisation's IoT security needs to be improved. 11 per cent state that cyber-security defences have not been a priority and could be vastly improved.

For these reasons, the sector is already carrying out a range of activities to address digital security. Most popular amongst these is investing in new security technologies, a change that has been made to address IoT security concerns by over half (51 per cent) of respondents, rising to 59 per cent in the rail industry. The other most common security measures include training employees on IoT (48 per cent) and the creation of an internal IoT security policy (42 per cent).



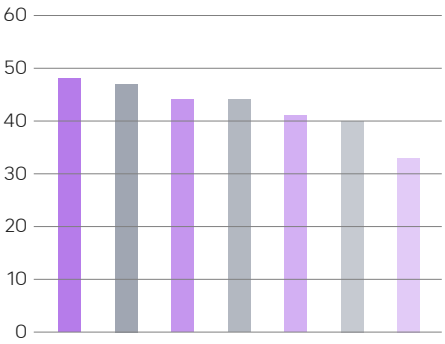
Which of the following statements are accurate regarding the security of your IoT projects?

- We have robust cyber-defences
- Our defences are good but could be stronger
- We need much better cyber-defences
- Our cyber-defences need to be vastly improved



What changes have you made to address IoT security concerns?

- Investing in new security technologies 51%
- Training employees on IoT 48%
- Creation of an internal IoT security policy 42%
- Communicating to customers on the use of IoT 41%
- Creation of an external IoT security policy for suppliers and partners 38%
- Hiring skilled staff 36%
- Upgrading existing security technologies 34%
- Partnering with a third party 27%
- Implementing a backup connectivity network 23%
- Securing physical assets such as sensor nodes 21%



What are your biggest IoT security challenges?

- Insecure storage of data collected 48%
- Insecure/unencrypted edge networks 47%
- Potential mishandling/misuse of data by employees 44%
- Risk of external cyber-attack 44%
- Internal data regulation and compliance requirements 41%
- Poor network security 40%
- Supplier/partner data regulation compliance requirements 33%

INVESTMENT

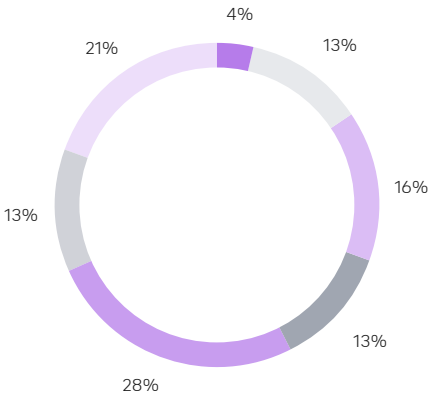
The average planned investment in IoT projects per organisation in the transport and logistics sector is $2,986,989 over the next three years. This is slightly above the average for all the industry sectors we surveyed, with rail companies planning on investing considerably more in the technology ($4,359,091 on average) compared with logistics companies ($2,529,621 on average). 21 per cent of the entire transport and logistics sample are also expecting to spend more than $4,000,000 on IoT technology investments in the coming years.

Unsurprisingly, the biggest transport and logistics companies (over 5,000 employees) have a much higher planned average spend of $6,656,154 compared with the smaller organisations we surveyed, with the planned IoT investment amongst the smallest businesses (251 to 500 employees) only $1,103,000. And North American transport and logistics businesses also have a much higher planned spend ($4,456,250) than all other regions.

However, despite these differences between sectors, geographies and different sized organisations, the fact remains that the proportion of transport and logistics IT budgets earmarked for IoT projects in the next three years is considerably higher than most other digital technologies. This includes cloud computing, next generation security and big data analytics. This is a trend that is particularly evident in the rail industry, where 11.7 per cent of budgets will be spent on IoT, and amongst the largest organisations surveyed in our research (over 5,000 employees), where 12.7 per cent is allocated.

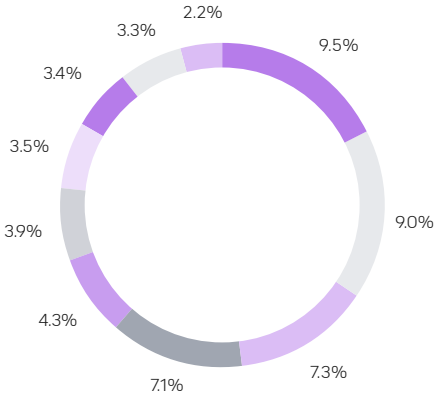
"Average planned investment in IoT across next three years $2,986,989."

Finally, perhaps the most encouraging sign of all is that the transport and logistics sector is reaching a level of IoT maturity, is the widespread awareness of the technology's potential to save businesses money, both in the short and long term. Currently, the average estimated saving for the typical transport and logistics business is 8 per cent, with this expected to rise to 14 per cent in 12 months, before eventually reaching 29 per cent in five years. Interestingly, it is those mid-sized transport and logistics businesses we surveyed (501 to 1,000 employees) that forecast the highest cost savings in the long term, expecting an average of 34 per cent in five years.



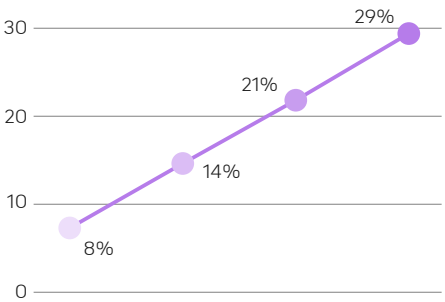
What is your planned investment in IoT projects in the next three years?

- $0 to £100,000
- $100,000 to $500,000
- $500,000 to $1,000,000
- $1,000,000 to $2,000,000
- $2,000,000 to $3,000,000
- $3,000,000 to $4,000,000
- $4,000,000 and above



What proportion of your IT budget will you spend on IoT projects in the next three years?

- IoT projects
- Cloud computing
- Next generation security
- Big data analytics
- Augmented Reality
- Machine Learning
- Virtual Reality
- Blockchain
- Cognitive AI
- 3D Printing



What proportion of your organisation's costs are saved/going to be saved from IoT projects?

Currently	8%
In 12 months	14%
In 3 years	21%
In 5 years	29%

HOW MATURE IS IOT AT YOUR ORGANISATION?

Inmarsat's free IoT maturity tool helps you compare your organisation's IoT maturity with our respondents and your competitors. Your personalised report also explains what you need to do to improve your score.

www.inmarsat.com/iotmaturitytool

REPORT ISSUED BY INMARSAT

99 City Road
London, EC1Y 1AX
United Kingdom

inmarsat.com/enterprise