TELECOM TV

SPONSORED BY

FORTINET

5G SECURITY SURVEY REPORT

LEVERAGING SECURITY TO CAPTURE THE 5G BUSINESS MARKET

IN ASSOCIATION WITH

HardenStance

ETSI

5G SECURITY

Leveraging Security to Capture the 5G Business Market

A TelecomTV survey in association with HardenStance and ETSI
Sponsored by Fortinet

INTRODUCTION

This TelecomTV survey for Fortinet asked telecom sector respondents for their perspectives on the evolution of the 5G market in enterprise services as well as the security requirements and security business models needed to support those enterprise services.

In total, 80 respondents completed the survey during the early months of 2020, with more than one third coming from the network operator/service provider community and a further quarter from the hardware/software systems vendor sector. (Details can be found on the final page of this report.)

This report comprises an Executive Summary, an analysis of the results of each survey question and details of the respondents' demographics.

The survey was researched, devised and written up by Patrick Donegan, Founder and Principal Analyst with industry analyst firm HardenStance. HardenStance provides trusted research, analysis and insight in telecom and IT security, and focuses a lot of its research on the intersect of the telecom and cyber security sectors.

EXECUTIVE SUMMARY

- The telecom industry is remarkably bullish about the prospects of growing ARPU with 5G: Almost 90% of respondents consider it likely that business ARPU will grow.

- Nearly three quarters of respondents believe that use cases tailored to unique vertical industries are either critical or very important to success in 5G.

- Transport, logistics, automation, manufacturing and healthcare are considered the most promising vertical industries for 5G enterprise use cases.

- During the next 5 years, telecom sector respondents expect roughly half the spend on enterprise use cases of 5G to go to private 5G networks and the other half to network slices managed by the operators. Since they also expect operators to build and operate roughly half the private 5G networks, respondents expect telcos to build and operate the network for three quarters of the total market in vertical industry 5G use cases.

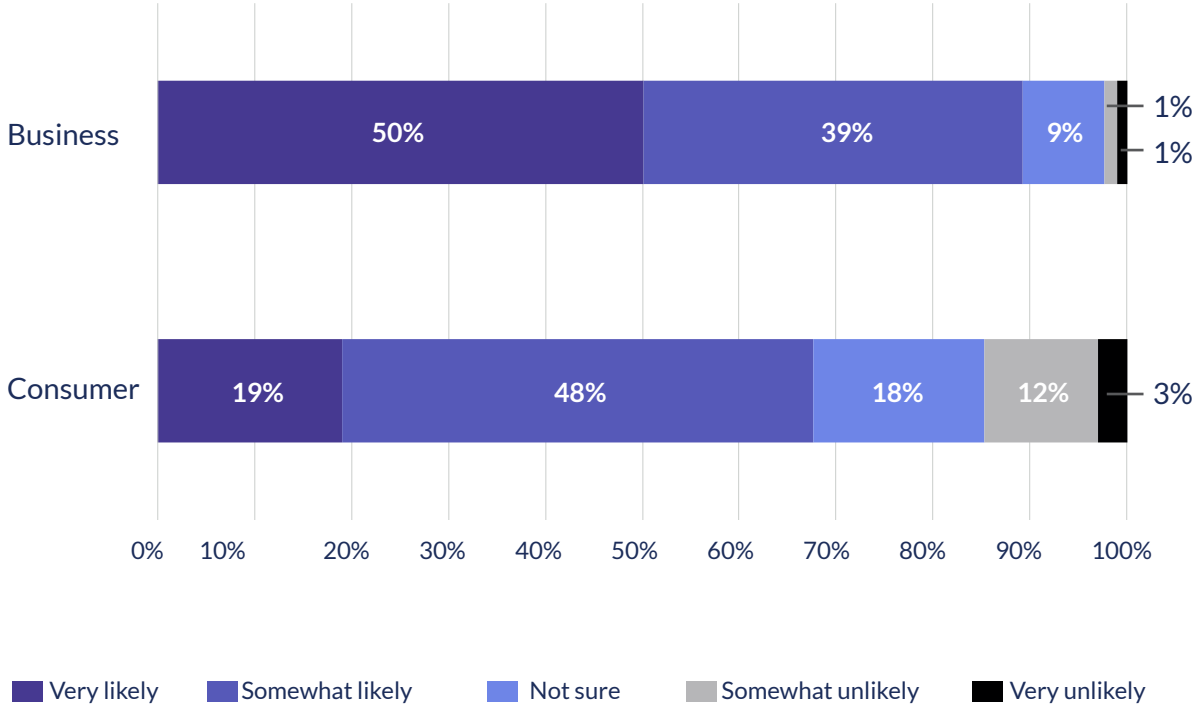
- More than 80% of survey respondents consider 3GPP's security features to be nothing more than a baseline for the security features needed to serve the 5G market.

- More than half of respondents believe telcos should offer enterprises a shared responsibility model for the supporting security services required for vertical industry use cases.

- The telecom sector thinks of the big cloud providers more as partners than as competitors in the 5G ecosystem: 44% of respondents consider the cloud providers to be partners or mainly partners; 29% consider them competitors or mainly competitors; and 28% consider them to be both in equal measure.

Those are the key takeaways – now let's look at the specifics, question by question.

IN THE COMING YEARS, HOW LIKELY IS IT THAT MOBILE OPERATORS WILL LEVERAGE 5G TO GROW ARPU YEAR ON YEAR FROM BUSINESS AND CONSUMER USERS RESPECTIVELY?

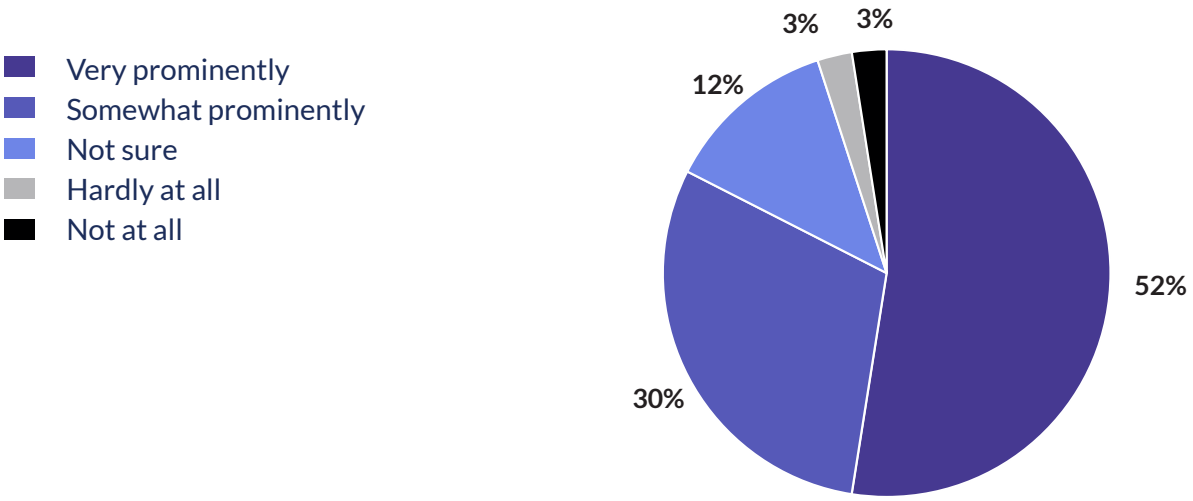


In general, the telecom industry is remarkably bullish about the prospects of growing ARPU (average revenue per user) with 5G. Almost 90% of respondents consider it likely that ARPU from business users will grow, more than half of which think business ARPU growth is "very likely". Two thirds of respondents even consider it likely that 5G will drive growth in consumer ARPU, although only 19% consider that "very likely".

> Almost 90% of respondents stated that an operator's security capabilities are either critical or very important

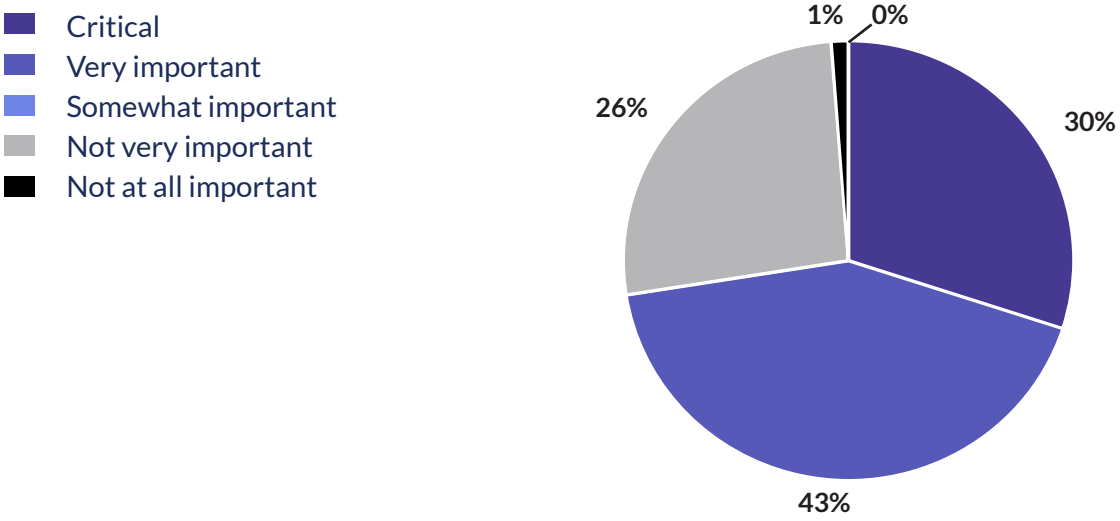
TO WHAT EXTENT WILL CONNECTED IoT 'THINGS' – NOT JUST SMARTPHONES, LAPTOPS AND TABLETS – FEATURE IN 5G USE CASES FOR BUSINESS CUSTOMERS?

Nearly everyone expects IoT 'things' to feature prominently in business use cases for 5G. More than half of respondents expect IoT 'things' to feature very prominently, another third expect them to feature somewhat prominently. Monitoring millions of different devices with different profiles in terms of performance, bandwidth and security requirements at scale creates a major challenge for telecom operators.



TO WHAT EXTENT IS SUCCESS IN 5G DEPENDENT ON USE CASES THAT ARE TAILORED TO UNIQUE VERTICAL INDUSTRIES AND WHICH OPERATORS CAN SELL TO MANY BUSINESSES WITHIN THOSE VERTICAL MARKETS?

Nearly three quarters of respondents believe that use cases tailored to unique vertical industries are either critical or very important to success in 5G. That's quite a data point. In terms of serving the business market with mobile services, the message is stark – no more business as usual. Operators that stick to the 3G and 4G model of delivering more or less the exact same 'plain vanilla' services to one business customer as the next will not succeed. The capabilities of the 5G ecosystem provides telecom operators and other actors with tools to customize services to unique business requirements on an unprecedented scale. Those that can exploit those tools have a chance of succeeding: Those that can't, don't.



WHAT DO YOU CONSIDER TO BE THE TWO MOST IMPORTANT INDUSTRIES THAT MOBILE OPERATORS SHOULD BE TARGETING WITH NEW BUSINESS USE CASES FOR 5G?

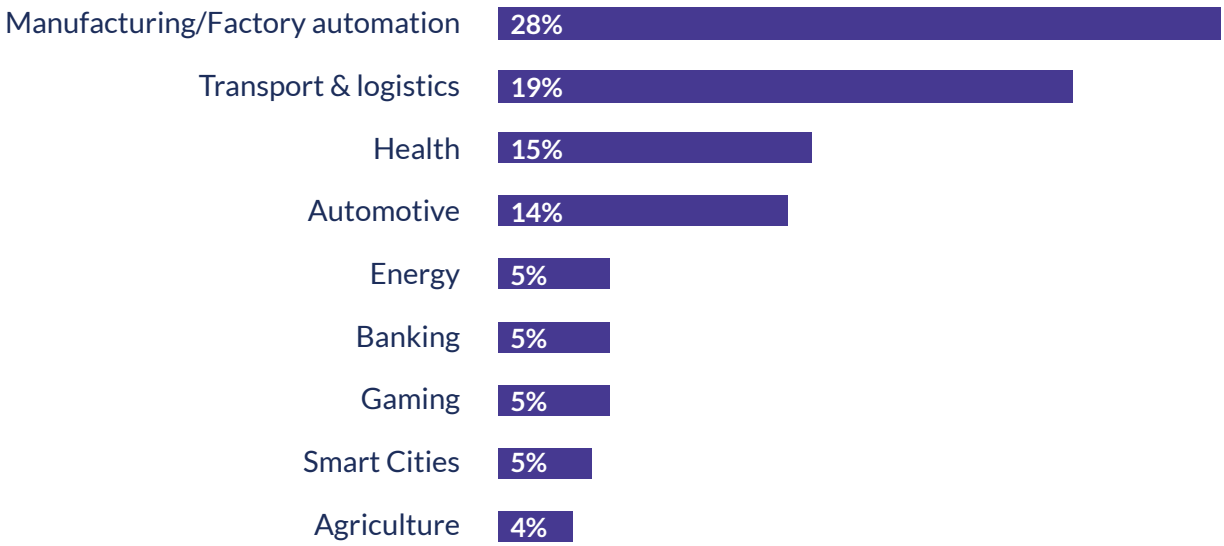
Rather than select from a menu of options, this question invited respondents to manually write in their own nominations of the two most important industries operators should be targeting with 5G use cases. Not surprisingly, the single biggest response category, with 26%, is comprised of respondents that either nominated their own esoteric pet project or replied 'Don't know'.

Those anomalous entries aside, three quarters of respondents nominated recognised industry verticals that tend to come up time and again in discussion of 5G use cases: These break down into two distinct groups of leaders and followers.

The leading group of most promising industries cited were transport, logistics, automation, manufacturing and healthcare. Telecom industry respondents clearly expect these use cases to scale relatively quickly. Manufacturing (factory automation) emerges as the most promising among these, nominated by 20% of respondents: That's unless you bundle together transport, logistics and automotive as a single category, in which case these three combined create the single biggest category, nominated by 25% of respondents.

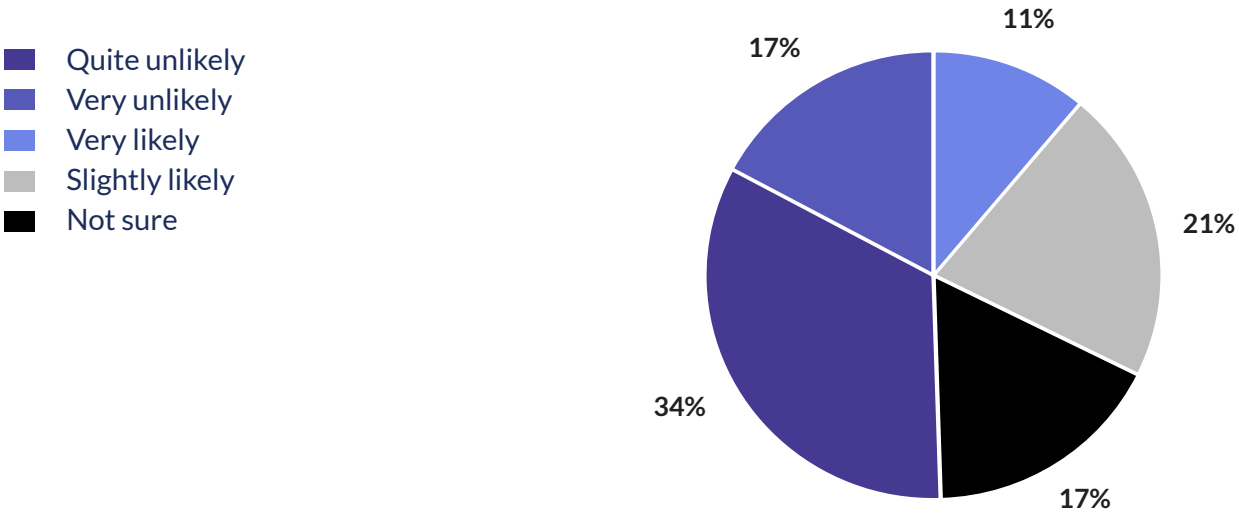
Unless you isolate automotive as its own category, rather than bundling it in with transport and logistics, the lowest level of support among the leading group of vertical industries is healthcare, nominated by just 11% of respondents. This probably reflects the diversity of intense regulations of this sector from one country to the next, and in some cases from one locality to the next.

Even though they also come up quite frequently in 5G use case discussions, our survey respondents hold out far less hope for industries such as financial services, agriculture, energy, gaming and smart cities: Fewer than one in twenty respondents identified any of these sectors as one of the two hottest 5G verticals.



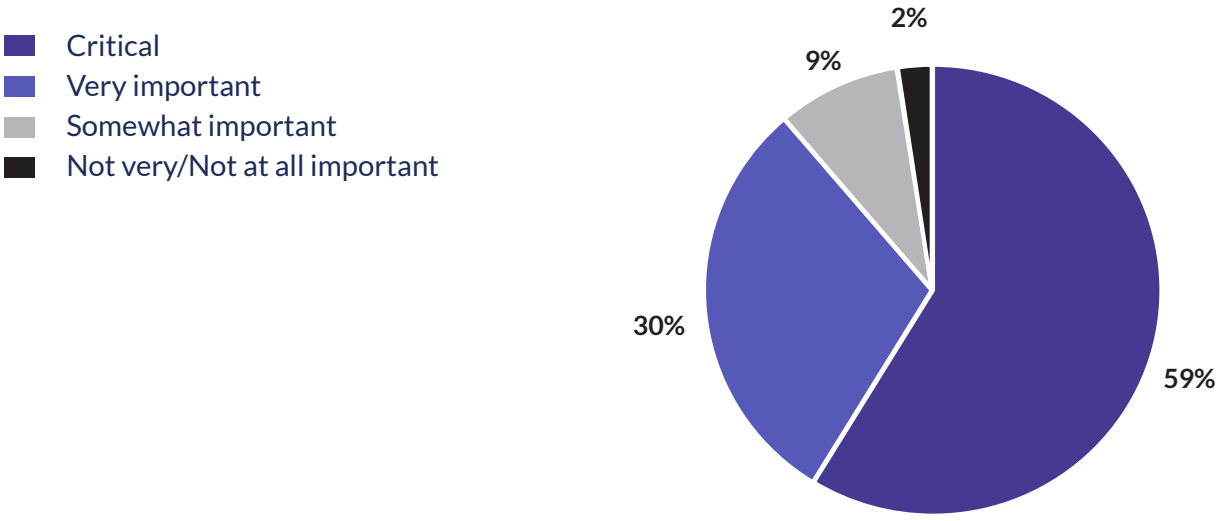
HOW LIKELY IS IT THAT MOBILE OPERATORS WILL BE ABLE TO GROW THEIR BUSINESS ARPU YEAR ON YEAR IF THEY FOCUS MAINLY OR ENTIRELY ON THE CONNECTIVITY LAYER OF THE 5G VALUE CHAIN?

Eliminating the 17% of 'don't know' respondents, 61% of the remaining respondents consider it unlikely that telcos can grow business ARPU if they confine themselves mainly, or entirely, to the connectivity layer of the 5G value chain. Of the 39% that think this can still be achieved, those who consider this outcome 'slightly likely' outnumber those that consider it 'highly likely' by two to one.



HOW IMPORTANT IS A MOBILE OPERATOR'S SECURITY VALUE PROPOSITION FOR SUCCESS IN VERTICAL INDUSTRY USE CASES OF 5G?

Respondents demonstrate a strong understanding of the importance of security. Almost 90% of respondents stated that an operator's security capabilities are either critical or very important, with those citing it as critical outnumbering those who think it very important by two to one. That respondents can make this assertion at such a high level isn't especially surprising: What's more interesting is to see how they anticipate that principle being put into effect at a more detailed level.



HOW DO YOU PERCEIVE THE ROLE OF THE 'SECURE BY DESIGN' FEATURES OF 5G SPECIFIED BY 3GPP, SUCH AS IMSI ENCRYPTION AND MUTUAL AUTHENTICATION?

More than 80% of survey respondents consider 3GPP's security features as nothing more than a baseline for the security features needed to serve the 5G market. Reflecting the diversity of potential 5G use cases, as well as different perspectives, respondents took different views as regards the level of dependency on additional security features. Depending on the use case, these could span public cloud, telco cloud and enterprise network domains.

Perhaps surprisingly, 20% of the total survey sample asserted that all use cases will require additional security features in addition to 3GPP's security features: That may be because they were thinking exclusively of advanced business use cases (which tend to need them) and not consumer services such as enhanced mobile broadband (which don't). In addition, 62% of all respondents asserted either that some, or most, 5G use cases will require additional security features.

A. They're not very important
B. They only provide baseline security. Some use cases require additional security features
C. They only provide baseline security. Most use cases require additional security features
D. They only provide baseline security. All use cases require additional security features
E. For the most part, these security features are all you need

> More than 80% of survey respondents consider 3GPP's security features as nothing more than a baseline for the security features needed to serve the 5G market

SHOULD MOBILE OPERATORS INSIST ON PROVIDING COMPREHENSIVE, FULL-STACK, END-TO-END SECURITY WITH 5G ENTERPRISE USE CASES?

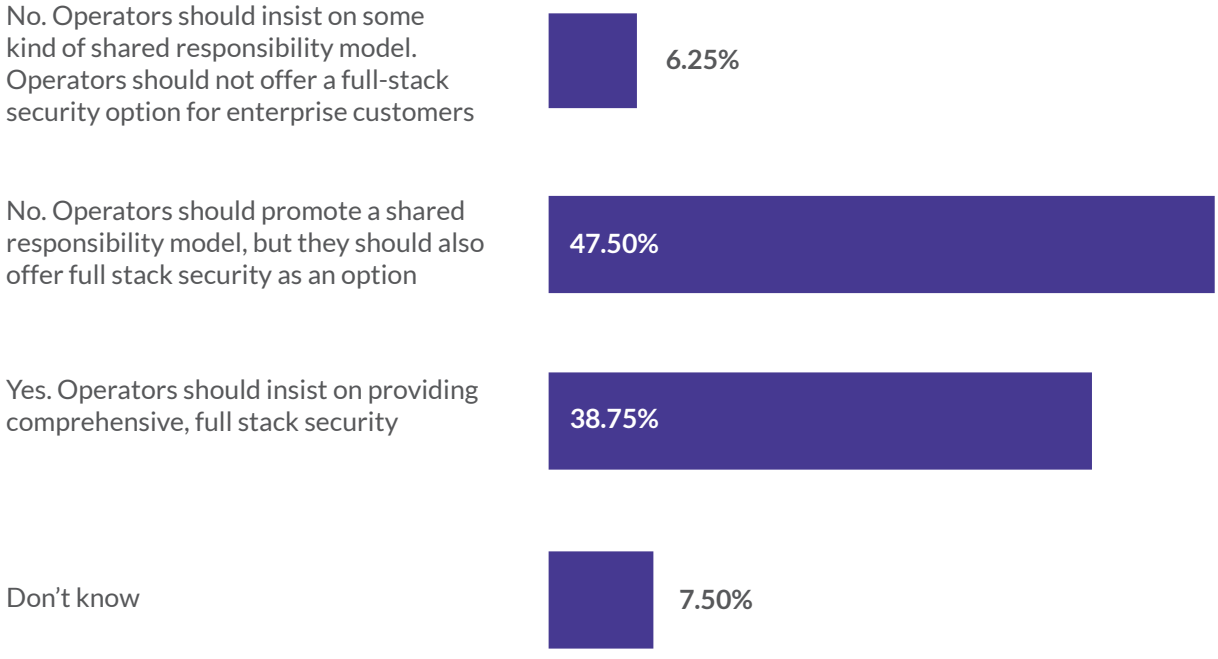
Depending on the specific vertical industry use case, enterprises expect to ensure the security of data at rest, in use and in transit across public cloud, telco cloud and enterprise network domains. Telecom operators have to consider exactly what role they want to play in that security ecosystem.

In this question, respondents yielded important evidence of a transition underway in how the telecom sector is thinking about security. It hasn't yet let go of the idea that it should be responsible for end-to-end security across vertical industry use cases, but at the same time it is becoming increasingly open to partnership models. These include shared responsibility models, such as those practised by the major public cloud providers. Here, the cloud provider (or telco) assures the security of the cloud infrastructure but the enterprise itself assures the security of their data and applications running in the cloud (including with tools made available to them by the host cloud provider).

The most revealing datapoint arising from this question is that 54% of respondents believe telcos should offer a shared responsibility model. However, nearly all those who support this approach believe that a shared responsibility model should be offered as an option alongside the alternative of comprehensive, full stack, end-to-end security. True to the traditional telco business model, fully 86% of respondents believe telcos should offer full stack security.

But reflecting the change in thinking that is underway, only 39% of all respondents adhere to the principle that telcos should insist on providing full stack security.

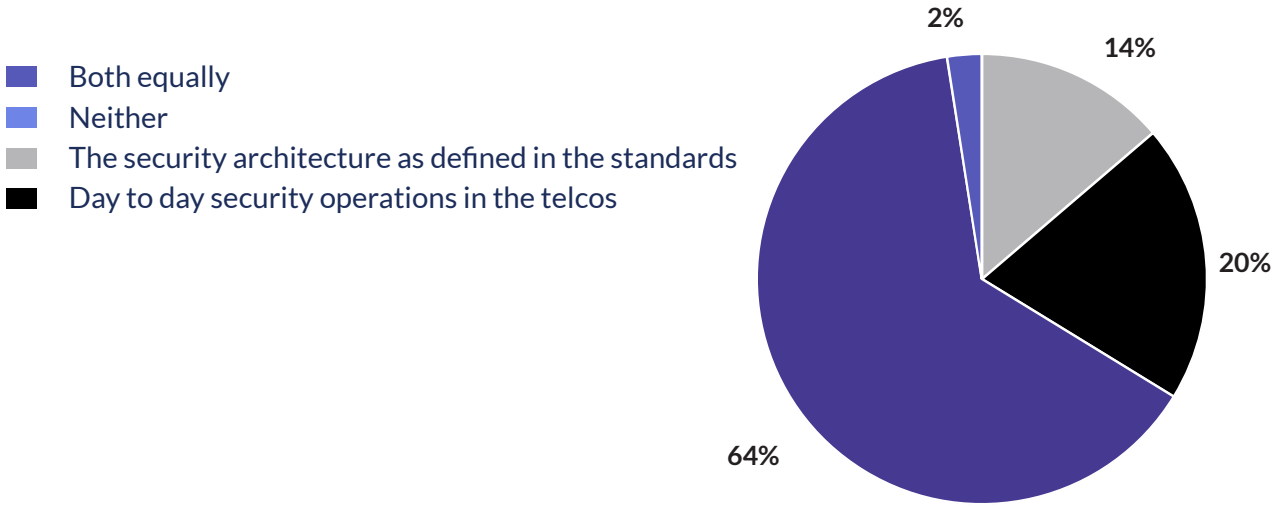
Hardly any respondents, just 6%, believe that telcos should directly copy the public cloud model and mandate a shared responsibility model.



WHICH OF THE FOLLOWING IS MOST IN NEED OF IMPROVEMENT IN THE COMING YEARS? THE SECURITY ARCHITECTURE AS DEFINED IN THE STANDARDS? OR DAY TO DAY SECURITY OPERATIONS IN THE TELCOS?

Most data breach incidents in telcos arise from flaws in security operations throughout a telco's organization. Only a minority arise from lack of implementation, or poor implementation, of the security architecture as defined in the standards.

Even if this day-to-day reality was appreciated by respondents, it doesn't appear to have much impact on their security thinking. Nearly two thirds of respondents believe the security architecture and security operations are both in equal need of improvement in the coming years. Of those who singled out one rather than the other, 20% pointed to security operations as the priority, while just 14% singled out the security architecture.



> True to the traditional telco business model, fully 86% of respondents believe telcos should offer full stack security

5G NON-STANDALONE (5G NSA) SERVICES ARE ALREADY WIDELY AVAILABLE, BUT TO WHAT EXTENT IS THE SUCCESS OF NEW 5G BUSINESS USE CASES DEPENDENT ON A 5G STANDALONE (5G SA) CORE WITH SERVICE BASED ARCHITECTURE?

Unsurprisingly, respondents overwhelmingly consider the capabilities of 5G SA to be important to new 5G use cases. These break down into 40% of respondents who believe hardly any incremental value can be delivered without 5G SA, and 49% who think it adds important additional capabilities rather than being critical.

Critically dependent – hardly any incremental value can be delivered until there is 5G SA
Somewhat dependent – 5G SA isn't essential but it does add important capabilities
Not very dependent – most of what an operator needs is already available with 5G NSA
Not at all dependent – everything an operator needs is already available with 5G NSA

> The lowest level of support among the leading group of vertical industries is healthcare, nominated by just 11% of respondents. This probably reflects the diversity of intense regulations of this sector from one country to the next

TO WHAT EXTENT IS SUCCESS IN 5G BUSINESS USE CASES DEPENDENT ON AN ADVANCED STRATEGY FOR THE NETWORK EDGE – E.G. WITH MULTI ACCESS EDGE COMPUTE (MEC)?

Similarly to the importance of 5G SA, respondents were clear in identifying the importance of an advanced edge strategy. The breakdown was also similar, as 42% believe that very little can be achieved without a supporting edge strategy, while 46% see 5G use cases as somewhat (rather than critically) dependent on advanced edge capabilities.

Critically dependent – very little can be achieved without a supporting edge strategy
Somewhat dependent – more can be achieved with a supporting edge strategy
Not very dependent – edge use cases are not that important
Not at all dependent – edge use cases are not at all important

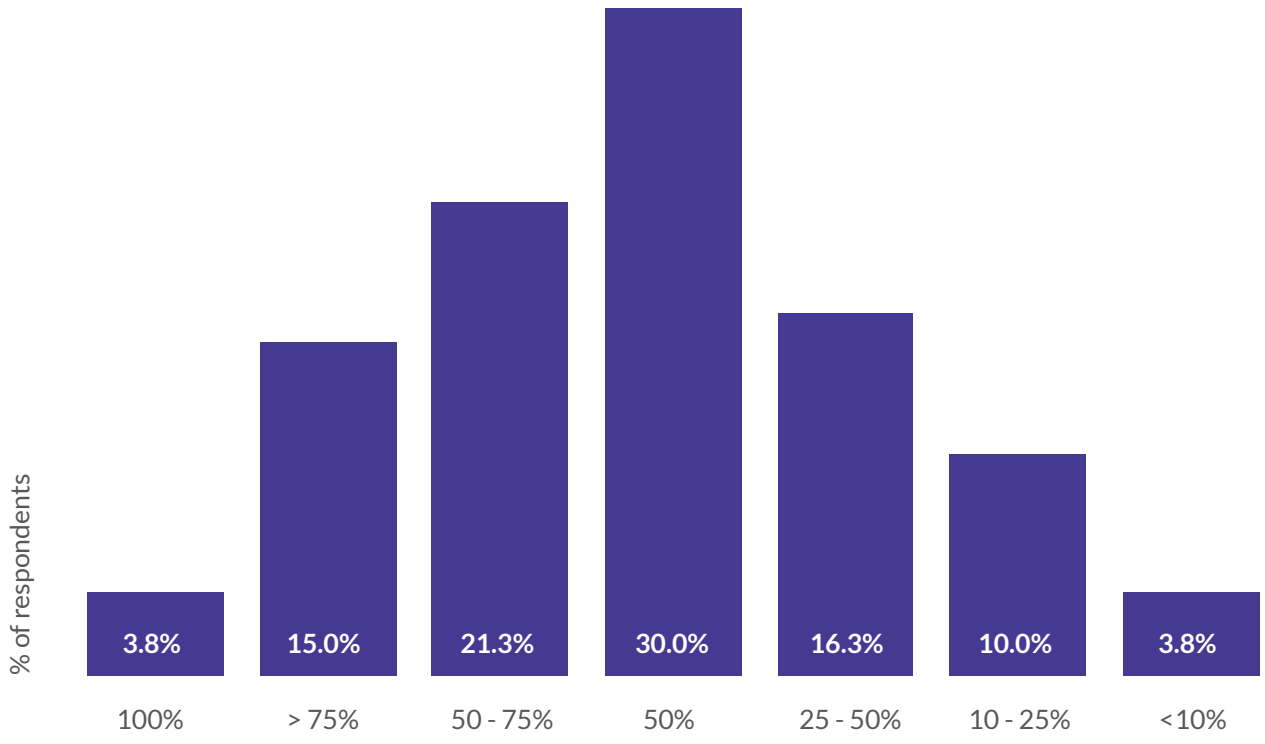
More than 50% of respondents expect IoT 'things' to feature very prominently

WHERE DEDICATED NETWORK RESOURCES ARE NEEDED, SPENDING WILL BE SPLIT BETWEEN DEDICATED 5G NETWORK 'SLICES' OF THE MOBILE OPERATOR'S 5G NETWORK AND A PRIVATE NETWORK BUILT USING THE BUSINESS CUSTOMER'S OWN SPECTRUM. OVER THE NEXT FIVE YEARS, WHAT SHARE OF THIS SPENDING WILL GO TO 'SLICES' OF THE MOBILE OPERATOR'S NETWORK?

The telecom sector is expecting roughly half the spend on enterprise use cases of 5G to go to private 5G networks, using the enterprise customer's own spectrum. Taking the mid-point for each estimate (e.g. 17.5% for the 10% - 25% category), multiplying it by the number of respondents, and dividing the total for all the categories by the total number of respondents, gets to a group forecast aggregated across all respondents that 53% of enterprise spend will go to operator slices, with 47% going to the buildout of private 5G networks.

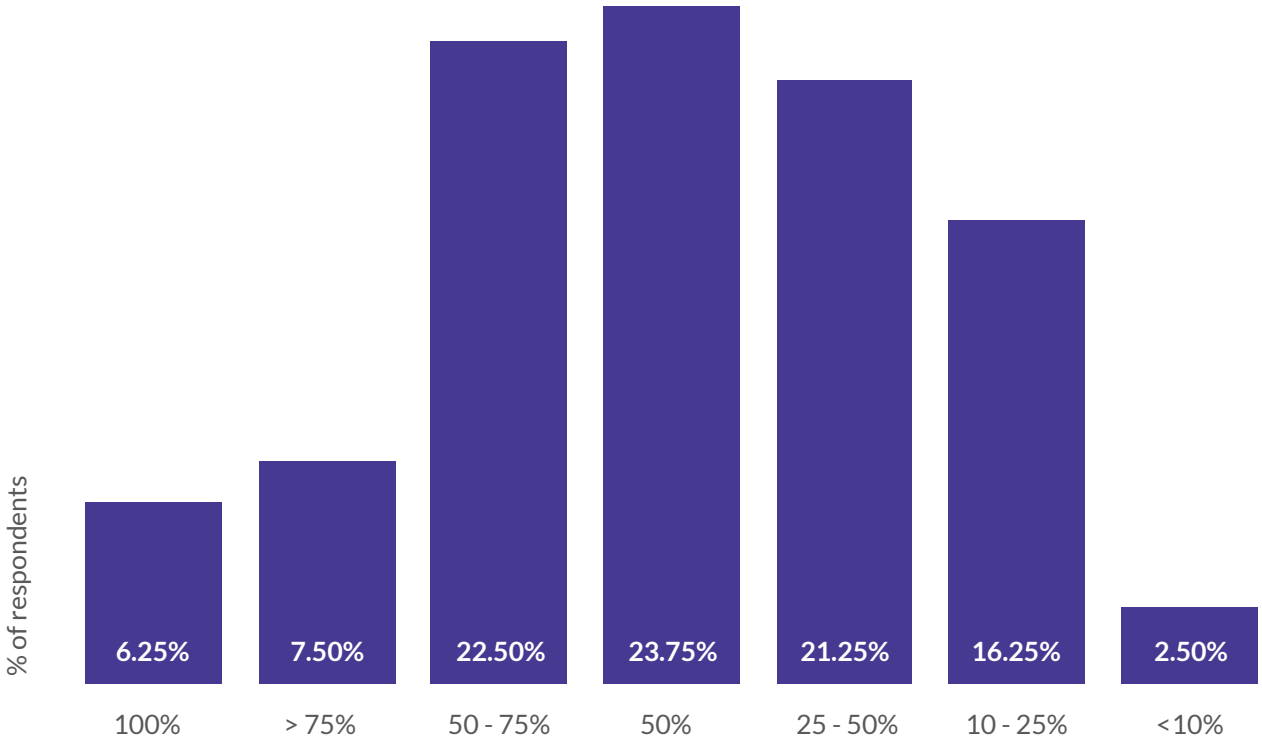
There's certainly a marked contrast between the current high level of activity around private 5G market and the reality that network slicing is at least a year or two away, and even then will be quite limited relative to long-term expectations: This appears to be baked into the thinking of the survey's respondents. That said, the question did ask respondents to address the five-year timeframe, so this response suggests that the telecom sector expects the early lead in deployment activity around the private 5G market to be sustained for longer than just the next few quarters.

This doesn't in any way mean that telcos should consider themselves excluded from almost half the 5G market for the next five years, though: As the data collected from the next question shows, our survey respondents consider telcos to be well placed to win around half the private 5G market as managed service providers responsible for building and operating many of those private networks.



IN THE CASE OF PRIVATE NETWORKS BUILT USING AN ENTERPRISE'S OWN SPECTRUM, SOME WILL BE BUILT AND OPERATED BY MOBILE OPERATORS, OTHERS WILL BE BUILT AND OPERATED BY THE ENTERPRISE CUSTOMER THEMSELVES OR BY A VENDOR. OVER THE NEXT FIVE YEARS, WHAT SHARE OF THIS PRIVATE NETWORK BUSINESS WILL GO TO MOBILE OPERATORS?

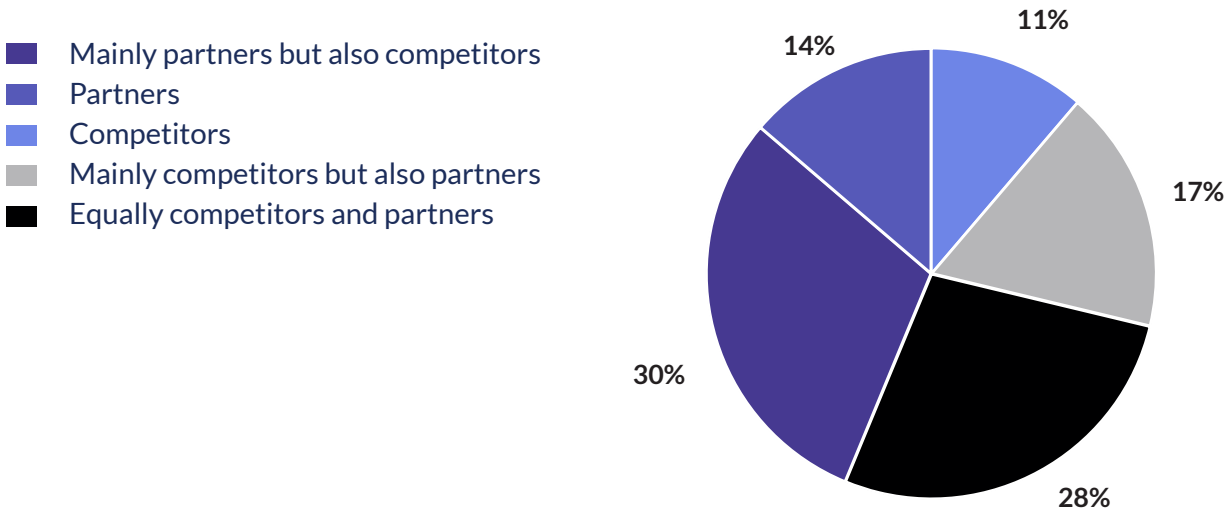
Using the same methodology as for the previous question, respondents expect telecom operators to win roughly half the business in building out private 5G networks on behalf of enterprise customers. Taking the responses to these two questions together, over the next five years, the survey respondents are expecting telecom operators to build out and operate around three quarters of 5G network infrastructure and services for enterprise use cases, spanning the operator's own network slices and private 5G networks. They expect that enterprises and their other ecosystem partners will account for an overall share of around 25% of that market.



THE BIG PUBLIC CLOUD PROVIDERS ARE TARGETING NEW ENTERPRISE SERVICES AT THE NETWORK EDGE THAT ARE GREATLY ENHANCED BY 5G. DO YOU CONSIDER THESE PUBLIC CLOUD PROVIDERS TO BE COMPETITORS OR PARTNERS FOR MOBILE OPERATORS IN THE ENTERPRISE SERVICES BUSINESS?

The appreciation of partnership models for advanced 5G use cases that emerged in the response to the question about full-stack, end-to-end security showed itself again in the response to this question: Not one respondent took the view that the big cloud providers are neither partners nor competitors in enterprise services – most respondents consider them to be a bit of both.

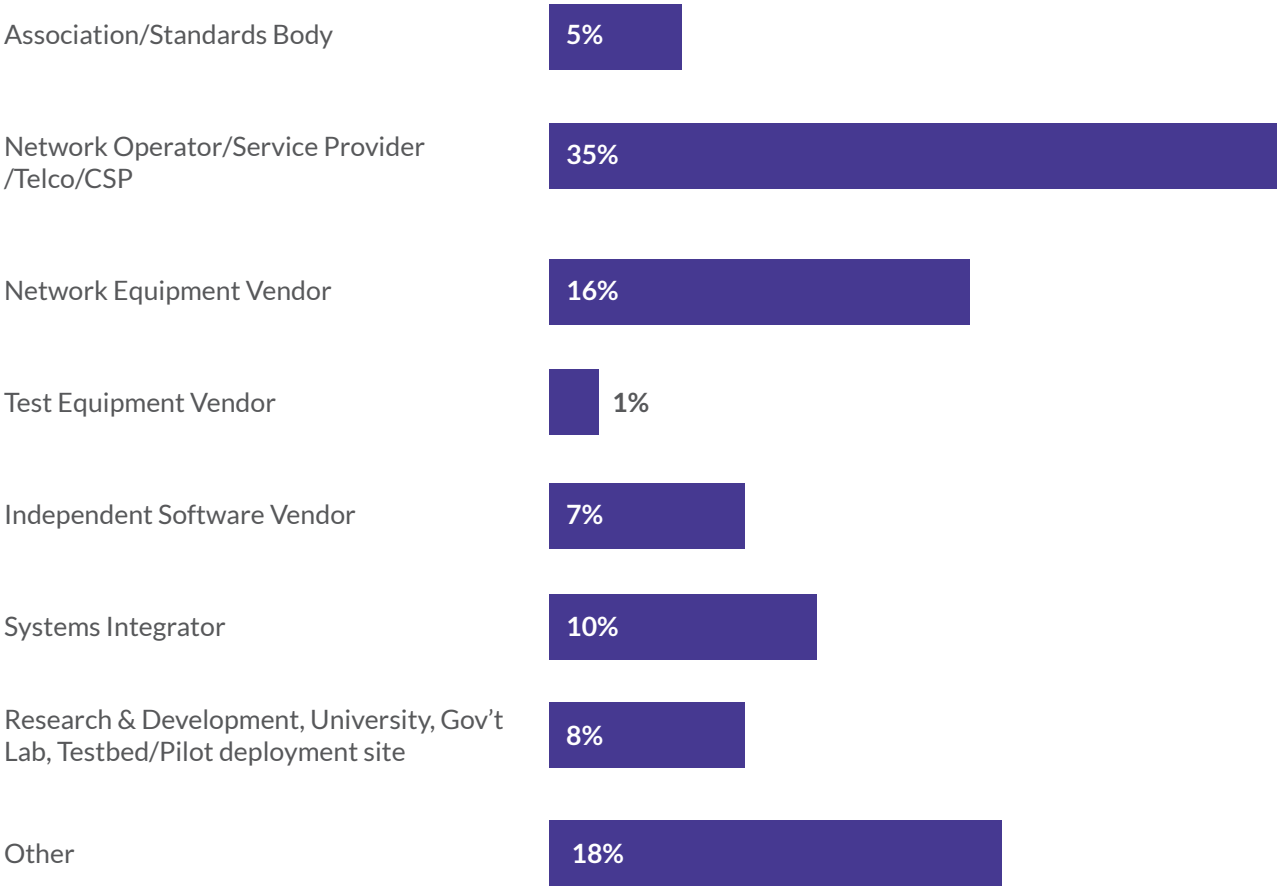
On balance, respondents think of cloud providers more as partners than as competitors to the mobile operators: 44% consider them to be partners or mainly partners; 29% consider them competitors or mainly competitors; and 28% consider them to be both in equal measure. Only 11% consider the public cloud providers to be out-and-out competitors.



> 29% of respondents consider cloud providers as competitors or mainly competitors

THE SURVEY RESPONDENTS

A total of 80 respondents completed the survey, of which 28 work at network operator/service provider organizations.



SUMMARY

If, as the survey results suggest, telcos are in a position to capture 75% of the 5G business market across their own network slices as well as building and operating private 5G networks, they are going to need to work with other ecosystem partners to get the security value proposition right. Baking 3GPP security features into their network and service infrastructure is a key baseline requirement but that alone isn't going to be enough. A lot of enterprise use cases for 5G will require many more security capabilities from the world of enterprise security to be layered in on top of that, especially now with the first 5G Stand Alone (SA) networks starting to be rolled out. Telcos should be looking at how their strategic intent here complements or competes with the big cloud providers, all of whom are expanding their security offers. Telcos should be thinking beyond just the traditional 'telco does it all' model. They should be considering shared responsibility models in which they co-create 5G security solutions with enterprises, cloud providers and other ecosystem partners.