

A D V A N C I N G

5G

SURVEY REPORT: JUNE 2023

SPONSORED BY



Introduction

Globally, 5G is forecast to overtake 4G/LTE as the dominant mobile technology with 47% of total mobile subscriber share in 2027, according to Omdia research house.

The adoption of 5G five years into its first launch is also expected to be much greater and more globally widespread than that of its predecessor.

Despite this growth forecast, and despite 5G deployments also ramping up in laggard markets such as in India, globally only 11% of all complete 5G rollouts are 5G standalone (5G-SA) deployments, according to Omdia. The 5G core unlocks the real capabilities it has to offer and that were promised by the industry. Such low SA penetration levels may be due to several factors including (but not limited to) the monetisation of service use cases, network function complexity, and integration requirements.

With 5G becoming more enterprise centric, simply relying on delivering a generic network and boosting investments through mobile data alone is no longer the most viable commercial route for telecom operators. While enhanced Mobile Broadband (eMBB) and Fixed Wireless Access (FWA) both will retain their relevance in terms of service monetisation, the industry is now at an inflection point in which there is a clear need for telcos to start delivering a network platform that can focus on the needs of enterprises while reaping the opportunities that 5G-SA presents.

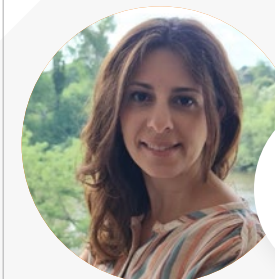
The current decade has seen an amalgamation of challenges including: a pandemic, a major conflict in Europe, global economic

crisis, political pressures across Asia and the Middle East, and much more. Amid such turmoil, security of digital services and products sits at the heart of life and more importantly business.

Against this backdrop, Telecoms.com Intelligence, in partnership with IEEE DiscoveryPoint for Communications and VIAVI, and with associate sponsorship from Blue Wireless, launched the annual 5G Industry Survey, which closed in late May 2023, to find out how the industry is advancing 5G. In so doing, it aimed to take stock at the progress 5G has made to date, where we are headed in terms of new trends and next steps, and to find out the views of the industry on the important topic of 5G security.

This report presents and analyses the survey data investigating the journey towards 5G-SA and its deployment strategies, the monetisation of services to drive greatest return on investment (ROI), top commercial capabilities, vendor partnership models, and best ways to address the challenge of keeping up with knowledge on new technologies and upskilling of resources. In the section dedicated to 5G security, we then go on to examine the impacts of security checks on user performance, the effects of operator security breaches which have compromised subscribers' personal data, the security of Open RAN versus traditional RAN infrastructures, and finally look to understand better the benefits of Secure Access Service Edge (SASE).

WRITTEN BY **ARMITA SATARI**
HEAD OF CUSTOM CONTENT,
TELECOMS.COM



telecoms.com

Demographic data

By the time the survey closed 120 industry professionals had completed it in total. Respondents represent a variety of organisations involved in 5G technology. The largest group consists of Communication Service Providers (CSPs) with nearly half the respondents (48%), this group includes mobile, fixed, and virtual operators. Hardware and software vendors (18%) and system integrators each make up the next largest groups (18%).

In terms of the job roles represented in our survey, there is a healthy mix from various positions within the industry. The largest group represented, with nearly a quarter of respondents (24%), is comprised of senior management such as CEOs, COO, CFOs, CTOs, VPs. About a fifth of respondents (21%) make up roles within sales and marketing. Professionals from mid-level management and engineering and development part of the industry combined make up over a quarter of the respondents (14% and 13%, respectively). About one in ten of respondents also come from the network operations side of telecoms.

With regards to respondents' geographic distribution, the largest

“With 5G becoming more enterprise centric, simply relying on delivering a generic network and boosting investments through mobile data alone is no longer the most viable commercial route for telecom operators.”

group is comprised of a European base with 38%. The second largest group is comprised of respondents across the African continent. This is an interesting observation as it differs greatly from the results of previous years where respondents from Africa were much smaller (2022: 6% vs. 2023: 20%), while North America (2023: 12% vs. 2022: 28%) typically made up the second largest group in previous iterations of our survey.

The increased participation from our African base and the decrease from North American may be

an indication of the stage of 5G progress across the respective regions. With more African markets launching 5G, there is naturally a stronger interest in insights and participation in research into the broader trends of 5G. Despite low ARPU and nascency of 5G in the region, examples of upselling are being [reported](#) from the continent, including 5G device bundles, segmented 5G plans, and 5G FWA to bridge the connectivity gap. On the other hand, with

North America being among the first regions to rollout 5G, priorities are increasingly shifting towards improved coverage and towards accelerating mid-band deployments of the technology. This may have caused a shift in focus towards more specialised insights.

Length of tenure is another demographic indicator measured by our survey over the years. Interestingly, this year we observe

a correlation between the number of respondents and length of tenure in the results. The largest group is made up of those with 25 years or more service in the industry (36%). This is followed by those with 20 to 24 years (20%), then 15 to 19 years (16%), while the smallest group makes up those with less than 5 years tenure in the industry with 3%.

For full demographic data please refer to the tables in our appendix.



New trends and next steps

To help gauge the progress on the different stages of 5G deployment, this year's survey opened by asking the respondents to indicate which 5G deployment phase they are currently engaged in.

It is worth noting that the 5G network can be built out as an overlay deployment integrated with a 4G core (i.e. non-standalone 5G also known as 5G-NSA), deployed as a new common core straightaway (i.e. 5G-SA), or for the 5G-NSA gradually replaced by 5G-

SA. However, to build a 5G network that can offer truly differentiated services and capabilities 5G-SA is required.

To begin with, the results indicate that our respondents see a clear value in deploying 5G-SA. Three in four survey participants¹ (75%) state that they either have already completed 5G-SA or will be rolling it out at some point in the next 4 years.

Drilling further down, while most respondents² have already completed 5G-NSA (59%), only 16% report they have already completed 5G-SA, and a fifth (20%) report they are actively rolling out 5G-SA. Meanwhile, a quarter of respondents (25%) are still rolling out non-standalone and have no immediate plans for standalone deployments. 24% of respondents

state they plan to rollout 5G-SA in the next 2 years, as another 15% plan to rollout SA deployments in the next 2-4 years. [Fig 1]

These trends are in line with the wider data being reported by the industry. With just 11% of all global live and commercial 5G network deployments comprising of 5G-SA, ongoing investments into 5G buildout will not rest in the near term. Further, global mid-band 5G penetration remains low, according to Nokia CEO Pekka Lundmark during its Q1 2023 earnings call.

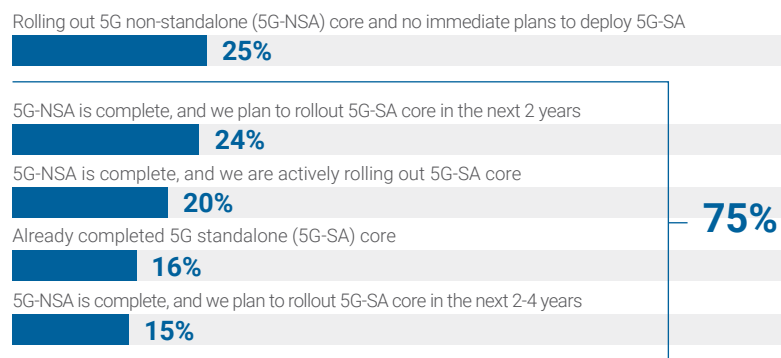
This indicates there is still a long way before 5G investments can slow down. Excluding China, only a fifth of all mobile stations are active in the mid-band range, reportedly. Even the more mature markets, such as those across North America which had started their investments much

earlier, are still expected to continue to deploy mid-band networks as the penetration of this frequency range currently roams around the 50% mark in that region.

When it comes to vendor selection in 5G core we observed two key approaches, with the largest group of respondents (32%) opting for multi-vendor partnerships with a dedicated system integrator to manage integration and interworking and the second largest group selecting multi-vendor partnerships managing the integration process in-house (30%). A single-vendor approach (19%) was the third likely route to vendor selection for our respondents in active 5G deployment.

FIGURE 1: 5G DEPLOYMENT STATUS

QUESTION: WHICH 5G DEPLOYMENT PHASE ARE YOU IN?



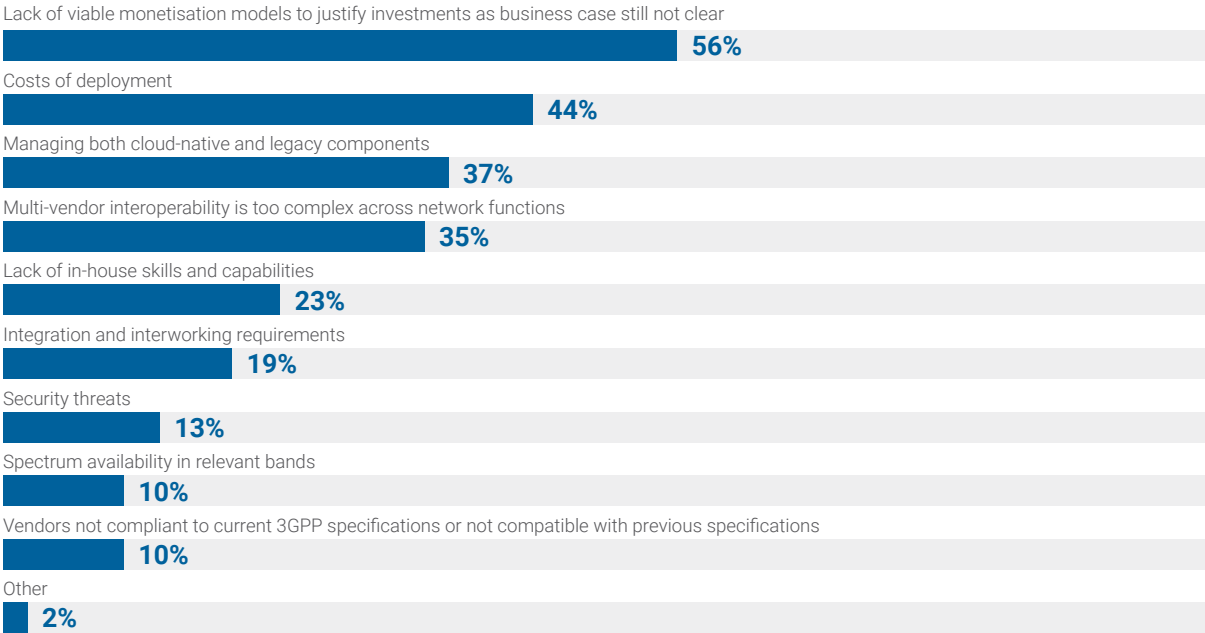
Base: Excludes respondents that selected 'not applicable'.

¹ Base = Excludes respondents who indicated this question is not applicable to them.
² Ibid

In rolling out and justifying the deployment of any new technology, it is inevitable that professionals will run into several challenges. This is also true when exploring the business case as well as during the initial stages of deployment and the phases of commercial operations. The main three barriers faced in the deployment of 5G-SA are: lack of viable monetisation models to justify investments as business case is still unclear (56%), costs of deployment (44%), and managing both cloud-native and legacy components (37%). The latter may be particularly true for those who will be making the transition from 5G-NSA to 5G-SA. [\[Fig 2\]](#)

Lack of viable monetisation models is particularly strongly reported by those from North America (67%), APAC (64%), and Europe (63%) regions. In Africa, cost of deployment is the most frequently reported barrier at 88%. Complex multivendor operability is naturally the top barrier for respondents from the vendor community (80%, both hardware and software), while system integrators struggle equally with the lack of monetisation models (75%) and cost of deployment (75%). Responses from the CSP community follow the

FIGURE 2: MAIN BARRIERS IN THE DEPLOYMENT OF 5G-SA
QUESTION: WHAT ARE THE MAIN BARRIERS YOU'RE FACING IN THE DEPLOYMENT OF 5G-SA CORE? (SELECT UP TO THREE.)



Base: Respondents in active 5G deployment; up to three answers permitted.

overall trend with more than half (56%) of the votes going to lack of monetisation models making the business case hard, cost of deployment (42%), and managing both cloud-native and legacy components (39%).

For [quite some time](#) now it has been clear that there is [no silver bullet](#) for 5G monetisation as the search for the 'killer app' continues.

Nonetheless, the capabilities unleashed by 5G-SA bring about a number of ways in which operators and partners can enhance service revenues and ROI. To this end, we asked our survey audience what they consider to be the top three 5G capabilities for monetising the network in the next two years.

Unsurprisingly, 5G enterprise private networks is the clear

“Three in four survey participants¹ (75%) state that they either have already completed 5G-SA or will be rolling it out at some point in the next 4 years.”

audience favourite monetisation capability with 59% of the votes. This finding is in accordance with our findings from previous studies and general industry consensus. Healthcare, manufacturing, and logistics and transportation are some of the key verticals some analysts deem as presenting unique opportunities for the telecoms industry.

The next frequently selected capabilities are FWA (43%) and eMBB (35%), the latter part of the core telecom services offered by mobile operators. Meanwhile, 5G FWA is increasingly being expected as the unsung hero. Especially in emerging markets with low fixed line penetration such as those across Africa and South America where mobile broadband already is the key access technology. Additionally, some mature markets such as the US may well choose to focus their 5G FWA deployments on areas with fewer high-speed broadband access technology alternatives available, such as rural areas with DSL as the alternative, or none at all. In the long term however, 5G FWA will have to compete with fibre build outs, those already underway and future investments, across many developed markets.

Other key capabilities for monetising 5G include network slicing (29%), massive machine type Communication and IoT (24%), Expanded support for non-traditional device types (21%), and network and API exposure (19%). [Fig 3]

Interestingly, this year's survey offers a new trend, deviating

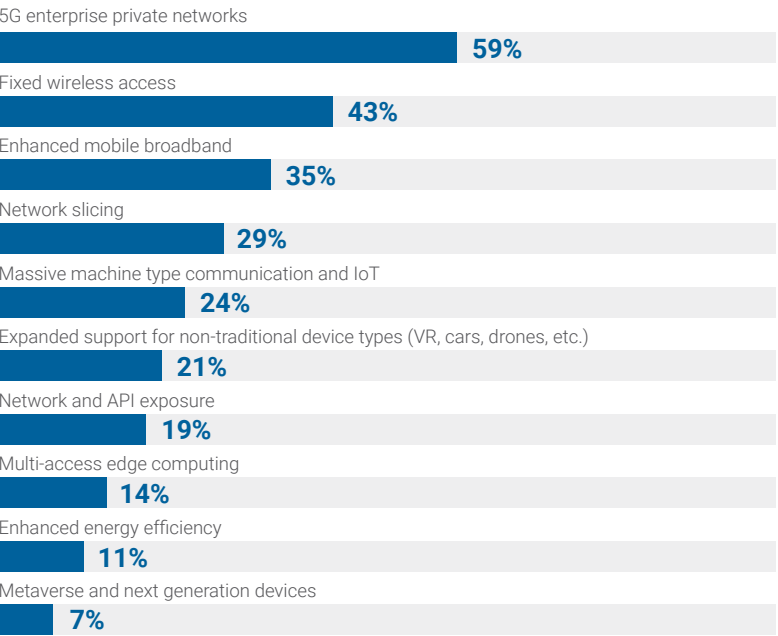
from previous iterations. Since the dawn of 5G, Multi-Access Edge Computing (MEC) has been considered playing a key role in addressing the needs of enterprises. And while this capability came up among the top three 5G features with greatest commercial significance in our survey of last year (33%, see

Q7 in the appendix of our [2022 survey](#)), it garnered only 14% of our responses to a viable route for 5G monetisation in this year's survey, indicating a slowdown in its growth potential.

This finding is also aligned with some market analysts' views of its growth. In a recent [statement](#) the Dell'ORO Group claimed the MEC market had failed to reach its initially anticipated potential (except in China) due to lack of applications with well-defined ROI, competition from hyperscale cloud networks as well as from 5G-SA private networks. The latter particularly is emphasized by our findings regarding the monetisation of network capabilities.

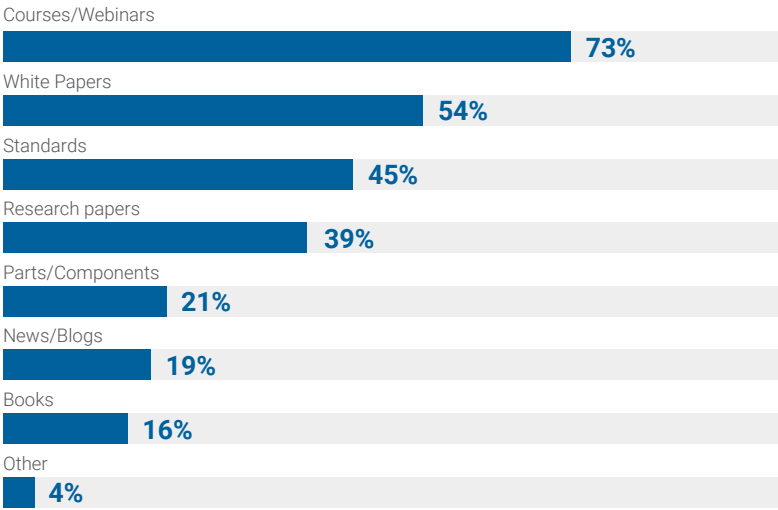
For many in the industry there is still a growing need to reskill and upskill their staff to handle new technologies – e.g. new applications and 5G's cloud-native systems and architecture – more efficiently and effectively. With this view, we investigated the types of information and insights that teams need to optimise their performance. By far the most frequently selected mode was courses and webinars with 72% of responses, followed by white papers (53%), standards (46%), and research papers (39%). [Fig 4]

FIGURE 3:
5G CAPABILITIES: MOST VIABLE ROUTES TO MONETISATION, NEXT 2 YEARS
QUESTION: WHICH 5G CAPABILITIES DO YOU SEE AS THE MOST VIABLE ROUTES TO MONETISING YOUR NETWORK IN THE NEXT TWO YEARS? (SELECT UP TO THREE.)



Base: All respondents; up to three answers permitted.

FIGURE 4:
INFORMATION SOLUTIONS NEEDED TO OPTIMISE TEAM PERFORMANCE
QUESTION: WHAT TYPES OF INFORMATION SOLUTIONS DOES YOUR TEAM NEED TO MORE EFFECTIVELY/EFFICIENTLY DO YOUR JOB? (SELECT ALL THAT APPLY)



Base: All respondents; multiple answers permitted.

These clearly highlight the need for more dissemination of insights across the industry. This notion of collaboration and dissemination is also further reinforced by the suggestions the audience made directly which included “market insights from other operators on their journey and challenges” and “real experience and benefits [resulting] from 5G deployment in industrial environments”.

For vendors and system integrators this means sharing success stories and best practices together with partner operators through webinars and whitepaper is a great way to earn credibility and showcase achievements. For operators sharing insights and success stories creates an opportunity to establish themselves both as market leaders and cheerleaders of the industry.



Sponsor's comment

IEEE DiscoveryPoint for Communications

The deployment of 5G capabilities continues to drive innovation, enhance productivity, and encourage new business models and services while pushing companies to remain competitive and adopt new standards or technologies.

In the case of 5G, companies are investing in the deployment of 5G-SA or 5G-NSA, and as this technology evolves, it is more important than ever for engineers and researchers to have access to cutting-edge and reliable information that applies to their workflows.

As noted in this report, healthcare, manufacturing, and transportation are some of the key categories to see new and unique opportunities for the telecoms industry. The best way for technical professionals to stay up to date with these demands and the evolving technology landscape is to have access to tools and resources that provide research and content in those industries. In addition, with

technologies often overlapping and expanding, technical professionals may also need to learn more about a topic that may be outside their expertise.

With robust tools such as IEEE DiscoveryPoint for Communications, engineers, and researchers can quickly and easily get the information they need to bridge any gaps in their knowledge and drive these 5G-related technologies forward. With access to courses, whitepapers, vital prior research, and industry standards, IEEE DiscoveryPoint for Communications provides a trusted source that engineers across industries can leverage to develop and confirm the skills they need to do their jobs.

About IEEE

IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. Through its Over 427,000 members in more than 190 countries, IEEE is a leading authority on areas ranging from aerospace systems, computers, and telecommunications to biomedical engineering, electric power, and consumer electronics, among other technologies.

IEEE publishes the science and technology research that is cited in patents more often than any other publisher. IEEE publishes approximately 200 annual journals and magazines and an average of 200,000 papers per year from sponsored in-person and virtual conferences held all over the world. IEEE also develops leading industry standards such as IEEE 802.11 (Wi-Fi), IEEE 2030 (Smart Grid), and the NESC®.

About IEEE DiscoveryPoint for Communications

IEEE DiscoveryPoint for Communications is an all-in-one platform built for engineers in industry to design and develop technology solutions. Curated by subject matter experts, this platform brings communications-focused information together from hundreds of vetted sources. Quickly find the technical information you

need and extract key insights from your results with machine learning. With IEEE DiscoveryPoint, spend less time searching and more time discovering solutions to optimize, improve, and innovate high-quality products.

Learn more at
discoverypoint.ieee.org

5G Security

Many in the industry agree on the need for disaggregation of the Radio Access Network (RAN), with the deployment of 5G often discussed as acting as a catalyst.

Such an open RAN approach is argued by proponents to enable mobile operators to leverage multi-vendor solutions, driving down costs and breaking the traditional vendor lock-in. Therefore, we aimed to better understand how open RAN fares in 5G security as compared to traditional RAN. The majority of respondents (58%) find more security concerns with open RAN as compared to traditional RAN infrastructure in 5G. Meanwhile, around a third of respondents (31%) say their security concerns are about the same with either RAN infrastructure. ^[Fig 5]

By splitting radio units and baseband software, the RAN can now be virtualised and more vendors can be introduced into one and the same network.

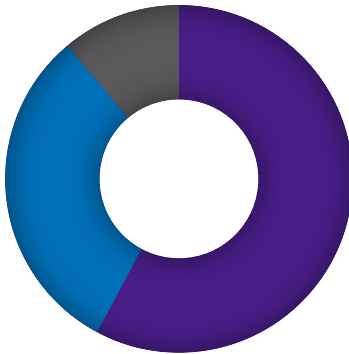
This introduction of open (and virtualised) RAN in a service provider infrastructure can present new waves of complexities. Having to stitch different pieces of technology together presents a higher risk of misconfiguration, exposing the RAN. Meanwhile, there is an increased risk of cyberattacks due to the larger attack surface this architecture presents. The lack of maturity in specifications is another concern, as laid out by a [report](#) from the Federal Office for Information Security in Germany. While the O-RAN Alliance has been working towards standards and specifications, the report states there is a lack in specificity in several areas of open RAN and that when it comes to security in particular little has been done to provide guidelines.

Drilling further down into RAN equipment security prevention, we asked our respondents for their views on adequacy levels of security testing done by RAN equipment vendors, Open Testing and Integration Centres (OTICs) and O-RAN Plugfests. Almost half of the

respondents (44%) believe the level of security testing being done by these organisations is appropriate. Meanwhile, a third (36%) are uncertain and only one in ten report there is little testing being done by RAN equipment vendors, OTICs and O-RAN Plugfests.



FIGURE 5: PERCEIVED SECURITY OF OPEN RAN
QUESTION: HOW DO YOU VIEW THE SECURITY OF OPEN RAN COMPARED TO TRADITIONAL RAN INFRASTRUCTURE IN 5G?



More security concerns.....**58%**
About the same.....**31%**
Less security concerns.....**11%**
Base = All respondents.

When it comes to user performance in 5G, organisations will aim to present optimum levels for their customer. This is especially important for capabilities such as latency and throughput where there is likely a service level agreement between a service provider and the enterprise customer. Meanwhile, security checks are a significantly important part of ensuring enterprises are ready to fend off security breaches and avoid cyberattacks. Yet the introduction of security checks, it is understood, can negatively impact user performance.

This view is confirmed by our audience responses. Most participants (74%) believe security checks will likely have a negative impact on user performance in 5G enterprise networks. But the relationship between enhanced security and performance does not have to be a mutually exclusive one. Introducing testing as a step prior to implementing security checks can enable CSPs to measure the effects of the security checks on performance indicators such as latency and throughput before committing to certain levels of checks.

This is also a view echoed by 42% of our respondents, who believe testing will allow them to strike the right balance between security and user

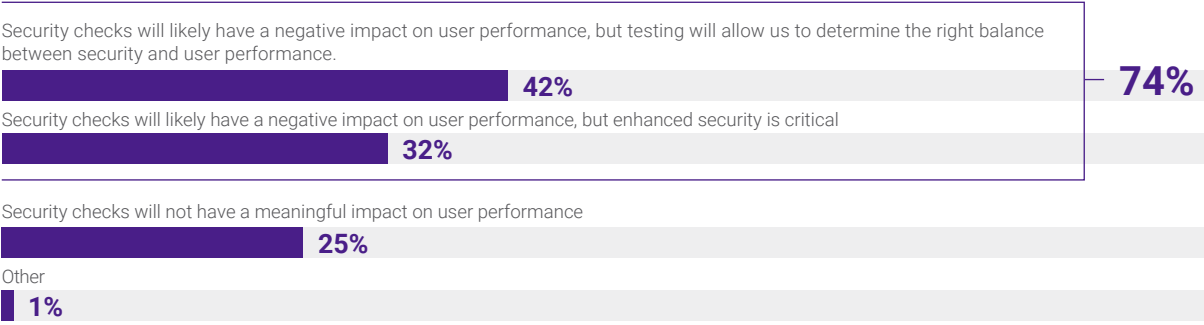


“Having to stitch different pieces of technology together presents a higher risk of misconfiguration, exposing the RAN. Meanwhile, there is an increased risk of cyberattacks due to the larger attack surface this architecture presents. ”

performance. Meanwhile, a quarter of respondents still believe there will be no meaningful impact on user performance. ^[Fig 6]

The security landscape in the 5G era is a changing one. As networks are

FIGURE 6: IMPACT OF SECURITY CHECKS ON USER PERFORMANCE IN 5G ENTERPRISE NETWORKS
QUESTION: WHICH STATEMENT BEST REFLECTS YOUR THOUGHTS ON THE IMPACT OF SECURITY CHECKS ON USER PERFORMANCE IN 5G ENTERPRISE NETWORKS?



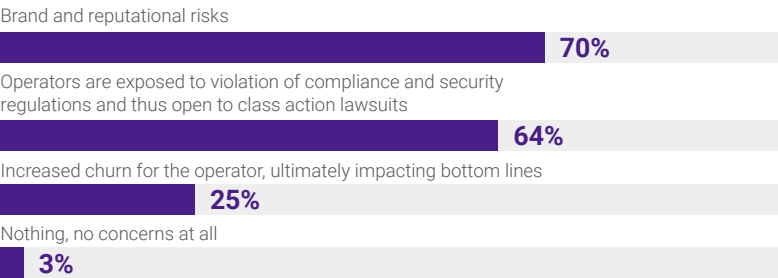
Base = All respondents.

increasingly more software-based, there is a growing complexity in implementing consistent security and a rise in the volume of attacks, meanwhile there is a fragmentation in the available security tools out in the industry. Combined, these transformations and challenges make it more difficult for security tools to defend against new threats, making the case for improved cybersecurity across the industry. Additionally, different governments around the world have different compliance policies and security regulations, making it more complex and resourceful for those telcos with operations across multiple countries or regions to keep up with updates and changes.

With many organisations holding large numbers of sensitive and identifiable data sets it is imperative for telecom operators, and their partners, to avoid security breaches that impact their customers’ privacy and consequently their business. With a growing number of data breaches in telecoms in recent years making such headlines for the wrong reasons – see [Syniverse](#), [T-Mobile US](#), and [Optus](#) for instance – we aimed to investigate what the top concerns for our industry stakeholders would be, if there were a security breach in a network operator that compromised subscribers’ personal identifiable information (PII).



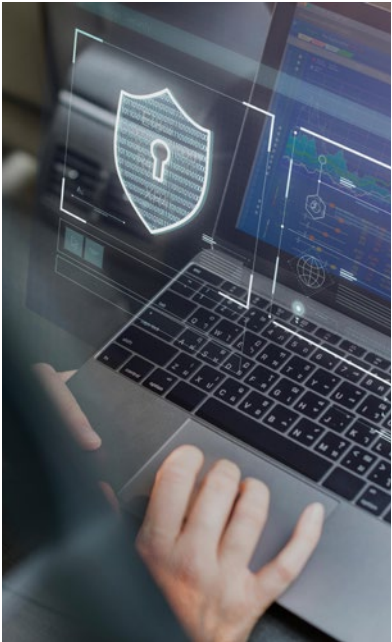
FIGURE 7:
TOP CONCERNS IN A SECURITY BREACH COMPROMISING SUBSCRIBER PII
QUESTION: WHAT DO YOU THINK ARE THE TOP TWO CONCERNS IN A NETWORK OPERATOR SECURITY BREACH COMPROMISING SUBSCRIBER PERSONAL DATA? (SELECT UP TO TWO.)



Base: All respondents; up to two answers permitted.

Our audience reaches a clear consensus with brand and reputational risks (70%), followed by exposure to compliance and regulatory violations resulting in vulnerability to class action lawsuits (64%) as the most two significant concerns. [Fig7]

Companies that make the headlines will further suffer from an increased churn and will be subject to additional costs to cover the damages that have already been done. Instead, investing in cybersecurity products and services, including managed security services, that have a strategic focus on cyber-resilience can not only offset churn and costs but also the devastating damages done through loss of reputation and brand value.



The advent of 5G and cloud has accelerated a shift away from data centres to a more dynamic mode of access and security available anytime from anywhere. Particularly in 5G enterprise, corporations’ data and privacy breaches can have a significant impact on many people and a company’s brand and reputation, as already discussed.

Against this backdrop, IT teams are faced with the hard job of finding the right balance between providing employees secure access, while also ensuring employee productivity is not hampered by features such as latency and throughput.

Secure Access Service Edge (SASE) architecture is a cloud-native framework, particularly relevant for addressing the need for remote connectivity e.g. to secure remote access to cloud-based applications and services. It can be adopted in both the public or private cloud domains or alternatively at enterprise edge.

With more employees now working remotely than ever before, we explored our audience’s view on SASE versus traditional Virtual Private Network (VPN). When asked to choose the top two primary benefits that SASE delivers

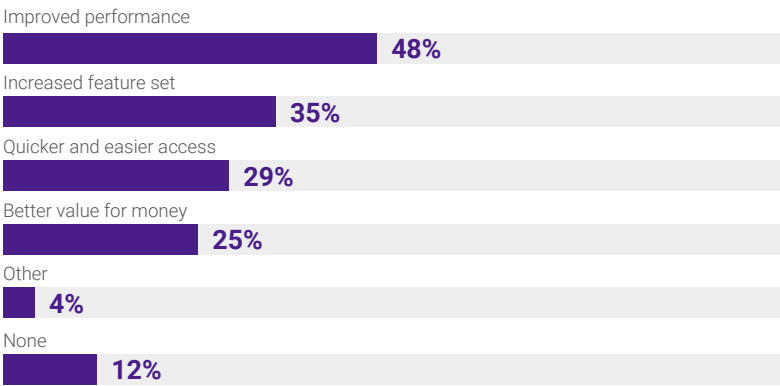
compared to VPN, our audience opted for improved performance (48%) and increased feature set (35%). Meanwhile though still a sizable minority (12%) believe there are in fact no benefits from SASE over VPN. [Fig 8]

Security is a domain within any organisation that requires deep technical expertise and CSPs have the right skillsets to become specialists in this area. In the current security landscape, SASE offers several technical benefits. Further, as SASE continues to mature it also offers a great opportunity for service providers

to capture a new revenue stream. This can be done through reselling of security vendor solutions to enterprises or via a partnership model with security vendors.

To achieve operational stability and service confidence, service providers can draw up on their own experiences adding further value and helping to demystify some of the challenges when transitioning between technologies. They can also employ testing measures using real traffic data, both at scale and with various cloud platforms, inserted malware, and scenarios where hardware fails to avoid pitfalls.

FIGURE 8:
PRIMARY BENEFITS OF SASE COMPARED TO VPN
QUESTION: WHAT PRIMARY BENEFITS DOES SASE DELIVER COMPARED TO VPN? (SELECT UP TO TWO.)



Base: All respondents; up to two answers permitted.



VI.AVI Solutions

Sponsor's comment

VI.AVI

5G is the first telecoms generation to introduce Open RAN disaggregation of networks, leading to a greater number of interfaces and vendors and thereby a larger attack surface.

5G is also the first telecoms generation facilitating cloud platform deployment of infrastructure and functionality, introducing massive IOT deployment, the separation of control and user plane as well as the widespread use of open source coding – all of which have increased the security attack surface beyond any previous telecoms generation. According to the accompanying 5G Security report - 58% of respondents feel Open RAN poses more security risks than traditional RAN infrastructure.

Two of the supposed 'killer applications' of 5G – Network Slicing and Private 5G – together

with Edge processing, Automation, introduction of the RIC and the adoption of AI/ML algorithms offer powerful technology advances but equally introduce a greater number of potential threats to the network.

The Cybersecurity market is growing rapidly with significant investment being spent to ward off the continuous threat of attack, for example the Dell'Oro Group recently forecast that network security sales will exceed \$150 billion US dollars globally over the next five years.

The 5G standards body 3GPP are doing their bit by taking security of 5G systems seriously with comprehensive specifications

insisting on zero trust networks. The Open RAN forum O-RAN Alliance have a dedicated Security Task Group charged with looking at how to design a secure network.

At VI.AVI, we believe cyber defense begins in the lab with thorough testing. VI.AVI has been securing network infrastructure, delivering a fully virtualized application and security validation solution to test and secure devices, networks and their services for over a decade.

About VI.AVI solutions

VI.AVI Solutions is a world leader in both network and service enablement and optical security performance products and solutions. Our technologies contribute to the success of a wide range of customers – from the world's largest mobile operators and governmental entities to enterprise network and application providers to contractors laying the fiber and building the towers that keep us connected.

Whether it be Distributed Denial of Service (DDoS) emulation to see what the impact of a DDoS attack has on network subscribers or failover testing for critical 5G Core systems or 5G Core embedded NGFW testing with real traffic and real cyber threats - the best way to prepare for and mitigate against cyber-attacks is with VI.AVI TeraVM Cybersecurity Test. VI.AVI offers a suite of 5G Security test products to ensure 5G systems are cyber safe before deployment. We also offer cybersecurity Test as a Service (Taas) running 3rd party vulnerability scanning tools on cellular network equipment. Defend your 5G network from the development phase, read more about VI.AVI 5G security test solutions at: Security Solutions for Wireless Operators - TeraVM VI.AVI

Learn more at
viavisolutions.com

Conclusion

Whether it be 5G-SA deployment plans or initial NSA network rollouts, our survey shows industry stakeholders still have a long way before efforts and investments of this generation of mobile technology can slow down.



While 5G deployments ramp up across the globe, the initial rollout of 5G missed the opportunity to provide telcos with a return to pricing power. As such, it is not surprising to see that in this next phase of the technology many stakeholders expect the monetisation of 5G to step up and significantly improve the return on investments made so far.

As many continue to debate the business case for 5G, including the deployment costs and complexities in the built-out of the network, our survey respondents agree on which 5G capability use cases they consider as the best ways to

monetise the network, at least in the near term.

Strong consensus is also indicated by our respondents regarding the security landscape of 5G. These include looming security concerns with open RAN versus traditional RAN, the best way to optimise the impact of security checks on user performance in enterprise 5G, the risks associated with security breaches involving subscriber PII, and the benefits of SASE.

Many of the trends identified in our survey are aligned with industry analyst market predictions and the wider discussions currently taking place across the telecoms industry.



A man in profile is holding a white wireless router with two antennas. In the background, there are server racks with blue and yellow cables. The scene is dimly lit, focusing on the man and the router.

Worry-free wireless connectivity

From urban sites to remote locations, Blue Wireless helps global enterprises and managed service providers harness the potential of LTE/5G networks, delivering reliable and flexible wireless connectivity in 80+ countries worldwide. www.bluewireless.com



Fredericus Arthur
SENIOR SOLUTION ENGINEER
BLUE WIRELESS SINGAPORE

SURVEY DEMOGRAPHIC DATA

Q1. Please select the type of company you work for (Base = All respondents)

Mobile / Fixed / Virtual Operators	48%
Hardware or Software Vendor	18%
System integrator / Consultancy	18%
Education Institute / Research or Consulting Firm	6%
Government / Regulator / Authority	3%
Cloud/Web Services / OTT	2%
Media / Entertainment	1%
Enterprise User	1%
Value-Added Reseller (VAR)	-
Other	4%

Q2. Which of the following best reflects your current job function? (Base = All respondents)

Corporate Management (CEO, COO, CFO, CTO, VPs)	24%
Sales / Marketing	21%
Mid-Level Management	14%
Engineering / Developer	13%
Network Operations	9%
Analyst / Research	4%
IT Management (CIO, VPs, Director of IT)	3%
IT Operations	3%
Administrative / Finance	3%
Other	6%

Q3. In which region is your company located? (Base = All respondents)

Europe	38%
Africa	20%
Asia / Asia Pacific	17%
North America	12%
Middle East	8%
South America	7%

Q4. How long have you worked in the telecommunications industry? (Base = All respondents)

Less than 5 years	5%
5 to 9 years	11%
10 to 14 years	13%
15 to 19 years	16%
20 to 24 years	19%
25 years or more	36%

NEW TRENDS AND NEXT STEPS

Q5. Which 5G deployment phase are you in? (Base = Excludes respondents that selected 'not applicable')

Rolling out 5G non-standalone (5G-NSA) core and no immediate plans to deploy 5G-SA	25%
5G-NSA is complete, and we plan to rollout 5G-SA core in the next 2 years	24%
5G-NSA is complete, and we are actively rolling out 5G-SA core	20%
Already completed 5G standalone (5G-SA) core	16%
5G-NSA is complete, and we plan to rollout 5G-SA core in the next 2-4 years	15%
Heavy industry	11%

Q6. What are the main barriers you're facing in the deployment of 5G-SA core? (Select up to three.) (Base = Respondents in active 5G deployment; Percents may reflect multiple answers)

Lack of viable monetisation models to justify investments as business case still not clear	56%
Costs of deployment	44%
Managing both cloud-native and legacy components	37%
Multi-vendor interoperability is too complex across network functions	35%
Lack of in-house skills and capabilities	23%
Integration and interworking requirements	19%
Security threats	13%
Spectrum availability in relevant bands	10%
Vendors not compliant to current 3GPP specifications or not compatible with previous specifications	10%
Other (please specify): Not applicable, Still on planning stage, N/A, No direct knowledge, not applicable	2%

Q7. Which 5G capabilities do you see as the most viable routes to monetising your network in the next two years? (Select up to three.) (Base = All respondents; Percents may reflect multiple answers)

5G enterprise private networks	59%
Fixed wireless access	43%
Enhanced mobile broadband	35%
Network slicing	29%
Massive machine type communication and IoT	24%
Expanded support for non-traditional device types (VR, cars, drones, etc.)	21%
Network and API exposure	19%
Multi-access edge computing	14%
Enhanced energy efficiency	11%
Metaverse and next generation devices	7%

NEW TRENDS AND NEXT STEPS

Q8. What is your approach to vendor selection in 5G core? (Base = Respondents in active 5G deployment)

Multi-vendor partnerships managing the integration process in-house	32%
Multi-vendor partnerships with a dedicated System Integrator to manage integration and interworking	30%
Single vendor approach	19%
Multi-vendor partnerships with a primary vendor managing the ecosystem for us	13%
Not applicable	6%

Q9. What types of information solutions does your team need to more effectively/efficiently do your job? (Select all that apply.) (Base = All respondents; Percents may reflect multiple answers)

Courses/Webinars	73%
White Papers	54%
Standards	45%
Research papers	39%
Parts/Components	21%
News/Blogs	19%
Books	16%
Other (please specify): training, real life, Market insights from other operators on their journey and challenges, Reveal experience and benefits results from 5G deployment in industrial environments	4%

5G SECURITY

Q10. How do you view the security of Open RAN compared to traditional RAN infrastructure in 5G? (Base = All respondents)

More security concerns	58%
About the same	31%
Less security concerns	11%

Q11. How would you characterize the level of security testing being done by RAN equipment vendors, OTICs and O-RAN Plugfests? (Base = All respondents)

Too much testing	10%
Appropriate level of testing	44%
Too little testing	10%
Don't know	36%

Q12. Which statement best reflects your thoughts on the impact of security checks on user performance in 5G enterprise networks? (Base = All respondents)

Security checks will not have a meaningful impact on user performance	25%
Security checks will likely have a negative impact on user performance, but enhanced security is critical	32%
Security checks will likely have a negative impact on user performance, but testing will allow us to determine the right balance between security and user performance.	42%
Other (please specify): participant did not specify	1%

Q13. What do you think are the top two concerns in a network operator security breach compromising subscriber personal data? (Select top two.) (Base = All respondents; Percents may reflect multiple answers)

Brand and reputational risks	70%
Operators are exposed to violation of compliance and security regulations and thus open to class action lawsuits	64%
Increased churn for the operator, ultimately impacting bottom lines	25%
Other	-
Nothing, no concerns at all	3%

Q14. What primary benefits does SASE deliver compared to VPN? (Select top two)(Base = All respondents; Percents may reflect multiple answers)

Improved performance	48%
Increased feature set	35%
Quicker and easier access	29%
Better value for money	25%
Other (please specify): Not sure, Increased security, don't know, Don't Know	4%
None	12%

