CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Monday 13 May 2019

OPTUS 5G COMING TO A SUBURB NEAR YOU

CommsWire (ISSN 2202-4549) is published by iTWire Pty Ltd. 18 Lansdown St, Hampton, Vic, 3188
CommsWire/Telecommunications Editor: Stan Beer
Staff writers: Peter Dinham, Alex Zaharov-Reutt, Sam Varghese. Columnist: John de Ridder
Advertising: CEO and Editor in Chief, Andrew Matler: andrew.matler@itwire.com • Tel: 0412 390 000

OPTUS REVEALS LIST OF FIRST 50 ERICSSON 5G SITE LOCATIONS

Optus has revealed the list of the first 50 5G site locations to be built by Ericsson across Sydney and Melbourne as part of its multi-vendor 5G rollout.

The sites will form part of Optus' plan to build and deliver 1,200 5G sites across Australia by March 2020, including in the ACT, Victoria, New South Wales, Queensland, South Australia and Western Australia.

NSW: 20 Suburbs

Greystanes
Macquarie Park
North Ryde
Marrickville
Peakhurst
Alexandria
North Ryde West
Dudley
Mosman
North Baulkham Hills
Enfield East
Castle Hill
Oatlands
North Ryde Business Park
Riverside Corporate Park
Carlton
Kellyville
North Sydney Central
Rydalmere
Panania

VIC: 30 Suburbs

Braybrook
Dandenong South
Greenvale Reservoir
Kensington
Springvale South
Rye Central
Preston East
Laverton West
Mt Martha
Noble Park South
Rosebud
Wantirna South
Mornington
Geelong West
Research
Coburg
Arthurs Seat
Rosebud East
Norlane
Campbellfield South
Brunswick
Mt Evelyn
Abbotsford
Fishermans Bend
Hoppers Crossing
Williams Landing
Croydon South
Maidstone
Noble Park
Reservoir North

Kent Wu, Optus' Head of Network Access Planning & Quality said "this is another significant milestone for Optus as we continue with our customer focused 5G roll-out plan. We are continuing to deliver a more dynamic and innovative 5G network for the benefit of our customers."

In January, Optus revealed plans for Optus 5G Home Broadband and Wu said Optus is now working with Ericsson to deliver a device for customers in these areas.

"We are working closely with Ericsson to conduct critical inter-operability device testing so that we can deliver a compatible 5G home broadband product to customers and open these sites up as part of our expressions of interest campaign.

"We are further demonstrating that our multi-vendor approach to Optus 5G will help to deliver a more dynamic and innovative 5G network for the benefit of our customers."

Wu said Optus has opened expressions of interest allowing customers to register their interest "to be amongst the first to experience 5G in selected suburbs in Australia".

To register interest, visit www.optus.com.au/5G and enter your suburb to check eligibility for the first phase of Optus 5G Home Broadband.

Peter Dinham

DEUTSCHE TELEKOM, ERICSSON CLAIM 100GBPS OVER MICROWAVE LINK

Swedish telecommunications equipment vendor Ericsson and Germany's Deutsche Telekom say they have achieved a "landmark" data transmission rate by consistently exceeding 100Gbps on a trial microwave link over 1.5km.

In a statement, Deutsche Telekom claimed the project, conducted at its Service Centre in Athens, represented a major technical breakthrough, achieving more than 10 times the throughput speeds compared to existing commercial solutions on similar 70/80 GHz millimetre wave spectrum.

The main technological advances included an 8x8 line-of-sight MIMO (LOS) with cross polarisation interference cancellation set-up using commercial MINI-LINK 6352 radios and a 2.5 GHz channel bandwidth in the E-band (70/80 GHz) able to transmit eight independent data streams over the radio path.

This corresponds to a breakthrough spectrum efficiency of 55.2 bps/Hz at peak. During the trial, carried out in mid-April, transmission rates measures were consistently above 100 Gbps, with telecom grade availability (higher than 99.995%), with peak rates reaching 140 Gbps.

Alex Jinsung Choi, senior vice-president of Strategy & Technology Innovation at Deutsche Telekom, said: “Advanced backhaul solutions will be needed to support high data throughput and enhanced customer experience in the 5G era.

"This milestone confirms the feasibility of microwave over millimetre wave spectrum as an important extension of our portfolio of high-capacity, high-performance transport options for the 5G era. In addition, it represents a game changing solution for future fronthauling capabilities.”

Per Narvinger, head of Product Area Networks, Ericsson, said: ”This trial signifies the successful establishment of true fibre capacities over the air using microwave.

"This means that microwave will be even more relevant for communications service providers in creating redundant networks as a back-up for fibre, or as a way of closing a fibre ring when fibre is not a viable solution.

"By carrying such high capacities, microwave further establishes itself as a key transport technology, capable of delivering the performance requirements of 5G.”

Deutsche Telekom said, apart from confirming the potential of microwave technology over millimetre-wave spectrum (70/80 GHz and above) as a 5G-and-beyond fronthaul and backhaul solution, the trial showed the importance of applying spectral efficient techniques, such as MIMO (multiple input, multiple output) on wireless backhaul technologies to address upcoming 5G radio access demands.

Sam Varghese

AVAYA LOOKING AT POTENTIAL BUYOUT AS 2Q2019 REVENUE DIPS

Unified communications vendor Avaya has seen a dip in revenue during the second quarter of fiscal 2019, with the company saying it earned US$709 million, a fall of 3.9% from the first quarter, and adding that it was exploring a buyout.

The company had told investors in February that it expected revenue for the second quarter to be between US$730 million and US$760 million.

President and chief executive Jim Chirico said in a statement: "Following the receipt of expressions of interest, the company has engaged J.P. Morgan to assist in exploring strategic alternatives intended to maximise shareholder value.

"The board has not set a timetable for the process nor has it made any decisions related to any strategic alternatives at this time. There can be no assurance that the exploration of strategic alternatives will result in any particular outcome.

"The company does not intend to provide updates unless or until it determines that further disclosure is necessary."

In March, a report said that Avaya was trying to effect a leveraged buyout from a private equity company, with its value, inclusive of debt, estimated at about US$5 billion.

A Bloomberg report a month later said it was planning an auction, after it had received unsolicited offers from potential purchasers. A ***Wall Street Journal*** article the same month said Avaya was holding talks to join its rival Mitel Networks in a stock deal worth more than US$2 billion.

"Our topline results and earnings fell short of expectations," Chirico said. "In response, we have implemented a number of corrective actions to drive improved performance.

"While I'm disappointed in our results last quarter, overall, I remain confident about our path forward given the momentum and traction we are seeing in many segments of our business including cloud, services and emerging technologies."

Avaya entered the public market in January after it emerged from Chapter 11 bankruptcy.

The exit from Chapter 11, which Avaya moved into in January the same year, was effected at a time when it had about US$6 billion in debt which it planned to cut down to US$2.9 billion.

Avaya was formerly a part of Lucent Technologies and became a separate unit in 2000.

Sam Varghese

INDIA INVESTIGATES GOOGLE ALLEGES ABUSE OF ANDROID DOMINANCE

The Competition Commission of India, the country's anti-trust agency, has issued orders for a probe into search and mobile operating system giant Google for allegedly abusing the position enjoyed by its Android mobile operating system to block its rivals.

Citing anonymous sources, ***Reuters*** **said** it had reported in February that the CCI had begun its probe last year.

In July last year, the European Union **hit** Google with a fine of €4.34 billion for an offence similar to the one the CCI is investigating.

Following initial investigations, the Indian anti-trust watchdog decided by mid-April that there was merit to the allegations and ordered a complete probe.

The sources told ***Reuters*** that the investigation would take about a year and the CCI would summon Google executives to appear before it in the months ahead.

The source of the complaint was unknown, the news agency said.

India has fined Google once before, **levying** a penalty of 135.86 crore rupees (about US$21.1 million) for "abusing its dominant position in online general Web search and Web search advertising services in India".

This was in February 2018, with the CCI saying at the time that the fine had levied following complaints by two websites in 2012: matchmaking website Bharat Matrimony (Matrimony.com) and the non-profit Consumer and Trust Society.

The CCI can fine a company up to 10% of its turnover in the previous three financial years for abusing a dominant market position.

New Delhi-based anti-trust lawyer Gautam Shahi told ***Reuters*** that Google's earnings from its Chrome browser and search engine could be taken into account when calculating the fine. These earnings are not disclosed by Google.

In March, the EU **fined** Google for alleged abuse of its AdSense advertising service, and told the company to fork out €1.49 billion (A$2.38 billion) for breaching EU anti-trust rules.

In June 2017, Google was fined €2.42 billion for **allegedly abusing** its search engine dominance to give illegal advantage to its own comparison shopping service. Google has appealed against the three EU fines.

Contacted for comment, a Google spokesperson told ***iTWire***: "Android has enabled millions of Indians to connect to the Internet by making mobile devices more affordable.

"We look forward to working with the Competition Commission of India to demonstrate how Android has led to more competition and innovation, not less."

Sam Varghese

PHISHING SECURITY THREAT FACING AUSTRALIAN BUSINESSES

Phishing is seen by almost one in two (44%) of Australian businesses as the biggest security threat they face, with ransomware, password and business email compromise continuing to beset organisations, according to a newly published survey.

And according to the survey commissioned by security intelligence firm LogRhythm, Australian chief information security officers continue to struggle to combat a rising climate of cybersecurity compromise, often taking weeks to detect and deal with security breaches.

The survey - conducted between February and April this year – found that more than half (55%) of respondents said they were able to detect their last security incident within hours, while 16% said it had taken them up to a week to detect their last security incident – and 7% had taken even longer.

“These delays really do raise serious concerns for Australian businesses, which since the introduction of the Notifiable Data Breaches (NDB) scheme, have been legally obliged to detect and report on breaches as rapidly as possible,” said Joanne Wong, Marketing Director Asia Pacific and Japan, LogRhythm.

“One might well conclude that if businesses cannot detect and evaluate a data breach, the consumer protections put in place by the NDB scheme offer scant chance of remediating breach damage.”

According to LogRhythm, the broad spectrum of responses to the survey confirms that security executives are facing a” steady barrage of attacks” that target access credentials, weaknesses in devices, and potential weaknesses in the extended connectivity chains that cloud computing and managed service provision have created.

When asked how they would meet the threats they face in 2019, respondents said that more advanced email and web security gateways, AI-based endpoint security systems, tighter control over user access rights, SIEM systems, application whitelisting, tools for secure coding, and offline backups were some of the critical tools being evaluated for improving their cyber posture.

"Ultimately, one of the greatest challenges IT teams face today is protecting their organisations from advanced and potentially costly attacks while operating with a limited budget and even fewer resources," said Wong.

"This is certainly not an easy task, but with the proper approach, it's also not impossible to protect your organisation's data and critical systems without impacting the agility of the business or increasing IT costs."

The survey also found that 52% of respondents are streamlining their security technologies to reduce the complexity of their environments for their people.

Just under half (48%) of these organisations are now turning to automation to assist employees transition away from security monitoring to focus on value adding tasks, the survey revealed.

In addition, other respondents said they were focused on implementing managed services, careful application of software updates, security awareness programs, incident response plans, and extensive training and upskilling of their people to support their employees.

According to LogRhythm, Australian companies still vary in maturity when it comes to adopting automation.

Half of respondents said they had applied automated incident detection and response (IDR) to less than half of their infrastructure, while 16% said they had successfully rolled out automated incident detection and response capabilities across their entire infrastructure.

"This suggests there is still a long way for Australian businesses to go when it comes to deploying the cybersecurity scalability to match the growing demands of digital transformation," LogRhythm notes.

When asked about budgets, 44% of respondents said their security budgets would increase by 5% or more in 2019 – although an almost equal percentage (46%) said their budget would stay the same.

LogRhythm says the survey found that security executives are facing a "steady onslaught of risks" in 2019 from malware and zero-day threats, identity theft, business email compromise, data loss, poor patching, credential theft, and data exfiltration.

In addition, there was a growing risk of nation state-sponsored attacks; web site hacks leading to theft of customer information; man-in-the-middle WiFi attacks; cryptojacking; cloud security breaches; malicious mobile apps; insecure third parties; and Internet of Things devices.

"This is certainly not an easy task, but with the proper approach, it's also not impossible to protect your organisation's data and critical systems without impacting the agility of the business or increasing IT costs," Wong said.

Peter Dinham