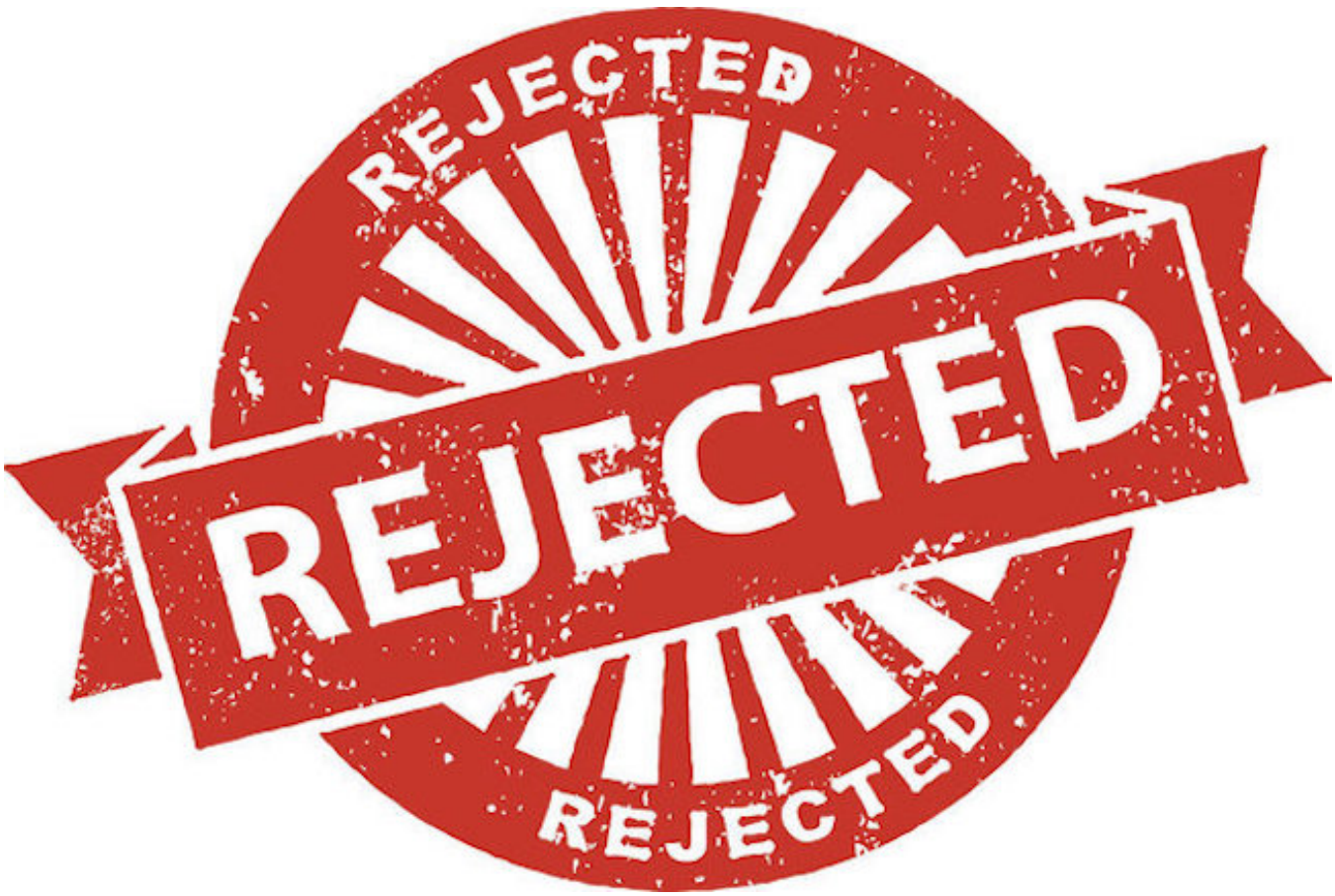
CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Monday 17 June 2019

VOCUS REBUFFED AGAIN AS AGL PULLS OUT OF BID



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

AGL ENERGY PULLS OUT OF BID FOR VOCUS COMMUNICATIONS

Australia's fourth largest telecommunications operator Vocus Communications has lost yet another potential acquirer, with AGL Energy announcing on Monday that it had withdrawn its non-binding, indicative proposal to buy the firm.

The **offer** was made on 11 June and was for all the shares in the company at $4.85 a share, meaning that the total bid would come to a shade over $3 billion.

AGL managing director and chief executive Brett Redman said in a statement to the ASX on Monday: “AGL is exploring investment opportunities across three focus areas: optimising our existing portfolio for performance and value, evolving and expanding our core energy markets offerings, and creating new opportunities with connected customers.

“We believe there will be material opportunities for AGL as energy and data value streams continue to converge and the traditional energy sector accelerates its transformation.

"The approach to Vocus reflected our view that the Vocus asset base has attributes that could support the execution of this strategy and benefit our customers.

“However, we are no longer confident that an acquisition of Vocus at the proposed terms would represent sufficient certainty of creating value for AGL shareholders. We would like to thank the Vocus board and management team for their assistance over recent weeks.”

Vocus CEO Kevin Russell commented: “As we have repeatedly said, this is a three-year turnaround. We have great confidence that our strategy and ability to execute our business plan will deliver significant value to our shareholders in the medium to long term.

"There is growing demand for our strategically valuable network assets and we have a substantial opportunity for Vocus Networks to gain market share. This is the core of our business. The Vocus management team will now be able to focus all of their attention on realising the opportunity that we have ahead of us.”

AGL had made a bid to buy Vocus last month, but backed out on 31 May when the terms of due diligence could not be agreed.

Prior to that, Swedish equity firm EQT Infrastructure **pulled out** of a bid for Vocus that valued the company at $3.3 billion or $5.25 a share.

In June 2017 **a report said** TPG Capital could team up with Vocus founder James Spenceley to examine a takeover in the event that the equity firm's bid for Fairfax Media failed.

The same month, American equity firm Kohlberg Kravis Roberts **made a bid** to buy Vocus for A$2.2 billion.

Vocus has suffered decreasing margins of its broadband business as NBN Co has made it difficult for RSPs to turn a profit. It wrote down its retail business by $1.3 billion in 2017.

Sam Varghese

MONTHLY AVERAGE LOSSES TO NBN SCAMS SOAR TO NEW LEVELS

Australians are losing more money to NBN scams, with consumers losing an average of more than $110,000 each month between January and May this year, compared with around $38,500 in monthly average losses throughout 2018 – an increase of nearly 300%.

The latest ***Scamwatch*** report from the Australian Competition and Consumer Commission (ACCC) shows that reported losses in 2019 are already higher than the total of last year's losses.

"People aged over 65 are particularly vulnerable, making the most reports and losing more than $330,000 this year," ACCC Acting Chair Delia Rickard said.

"That's more than 60% of the current losses.

"Scammers are increasingly using trusted brands like 'NBN' to trick unsuspecting consumers into parting with their money or personal information."

The ACCC reports that common types of NBN scams include:

- Someone pretending to be from NBN Co or an internet provider calls a victim and claims there is a problem with their phone or internet connection, which requires remote access to fix. The scammer can then install malware or steal valuable personal information, including banking details.
- Scammers pretending to be the NBN attempting to sell NBN services, often at a discount, or equipment to you over the phone.
- Scammers may also call or visit people at their homes to sign them up to the NBN, get them a better deal or test the speed of their connection. They may ask people to provide personal details such as their name, address, date of birth, and Medicare number or ask for payment through gift cards.
- Scammers calling you during a blackout offering you the ability to stay connected during a blackout for an extra fee.

The Commission cautions that it is important to remember NBN Co is a wholesale-only company and does not sell services directly to consumers.

“We will never make unsolicited calls or door knock to sell broadband services to the public. People need to contact their preferred phone and internet service provider to make the switch,” NBN Co Chief Security Officer Darren Kane said.

“We will never request remote access to a resident’s computer and we will never make unsolicited requests for payment or financial information.”

“If someone claiming to work ‘for the NBN’ tries to sell you an internet or phone service and you are unsure, ask for their details, hang up, and call your service provider to check if they’re legitimate. Do a Google search or check the phone book to get your service provider’s number, don’t use contact details provided by the sales person,” Rickard said.

Rickard also warns that consumers should “never give an unsolicited caller remote access to your computer, and never give out your personal, credit card or online account details to anyone you don’t know – in person or over the phone – unless you made the contact”.

“It’s also important to know that NBN does not make automated calls to tell you that you will be disconnected. If you get a call like this just hang up.

“If you think a scammer has gained access to your personal information, such as bank account details, contact your financial institution immediately.”

More information about NBN scams is available online at ***NBN Co***.

Peter Dinham

ASPI 'RESEARCHER' WRONG IN THINLY MASKED ATTACK ON HUAWEI

COMMENT: In a thinly veiled attack on the Chinese telecommunications equipment vendor Huawei Technologies, defence industry funded conservative think tank the Australian Strategic Policy Institute has managed to get most of its facts wrong.

Elise Thomas, who claims to be a researcher with **ASPI's** International Cyber Policy Centre, penned **an anti-Huawei op-ed** for the ***Australian Financial Review*** on Monday, and also looked to promote a so-called "**study**" done by the organisation about technology companies in China.

But in picking the numerous smart city projects being undertaken in different parts of Australia as her takeoff point, Thomas got her facts quite mixed up, claiming that such projects could be attacked by ransomware.

She cited the case of the US city of Baltimore, which has been hit by ransomware known as Robinhood, but appeared to be ignorant of the fact that it is the city's desktop systems, which run ancient versions of Windows, that have been affected.

Thus her lead-in, "City systems and infrastructures (sic) have already proven to be prime targets for hackers" made no sense as smart city devices do not run Windows.

Another brave attempt at being technologically literate, "The more connected our critical infrastructure and systems become, the more vulnerable they are to cyber attacks, including targeted hacks and global catastrophes such as WannaCry and NotPetya", again made no sense because both WannaCry and NotPetya are a Windows disease.

Perhaps Thomas was taking a leaf out of the book of her boss, Peter Jennings, who **put his foot deep into his mouth** by claiming, after the hack at the Australian Parliament, that the fact that users had been to change their passwords indicated that the breach was a serious one.

In reality, changing passwords after a breach is an indication that the investigators are fairly sure that there has been no deep intrusion into the system; it is the first bit of network hygiene, as even a junior sysadmin would confirm.

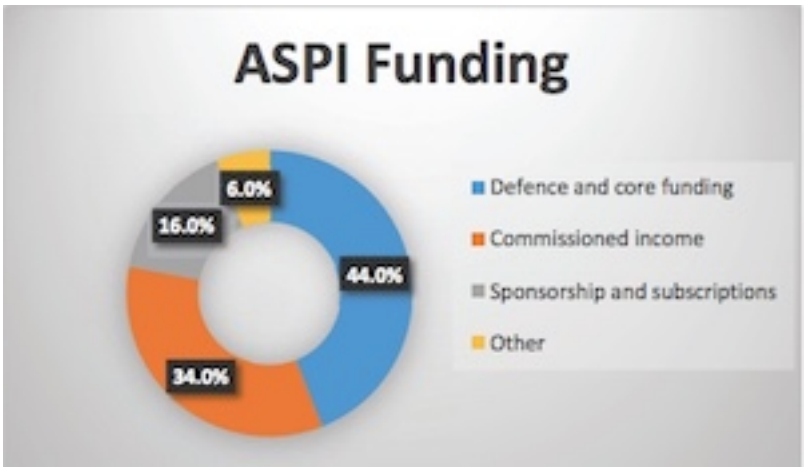
Australia's mainstream media often quotes people who work for ASPI, but never tell the public about the organisation's backers so that one can evaluate their public utterances. Not even the taxpayer-funded ABC does so.

But as ***iTWire*** has pointed out, ASPI's main sponsors are shipbuilder Austal, US defence contractor Lockheed Martin, Swedish defence company Saab, the Australian arm of American defence contractor Raytheon, MBDA Missile Systems, accounting firm KPMG and Jacobs, a global provider of technical, professional, and scientific services.

Its cyber policy centre is backed by French defence contractor Thales, Google, au domain namespace administrator auDA, security firm Palo Alto Networks, the Federal Government, Jacobs and encryption company Senetas.

With money pouring in from such sources, how can any organisation claim to be independent?

But back to Thomas, who by now has come to the meat of her article: Huawei is a bad company. But she defeats her own arguments, weak as they are, by first asking, "If Huawei is not trusted to supply 5G systems, why should it be trusted with other smart cities projects in Australia?" and then writing, "Huawei has not been involved in implementing smart city projects in Australia as far as is known".



After trying to find out which companies were supplying tech to the City of Darwin and failing, Thomas was apparently frustrated. So she gave vent to her frustration by guising it as public spiritedness: "It shouldn't be this difficult for citizens to find out what technology is being implemented, by which companies for what purposes, and what steps are being taken to ensure those systems are secure."

But if you told someone whose level of technical knowledge is apparently at the kindergarten level about measures taken to ensure network security, what is the chance he/she would understand it?

It would be a big waste of time – and maybe the officials in Darwin realised it.

Perhaps the senior folk at ASPI should look for a researcher who has a clue about technology; they are already exposed by Jennings and their financial ties, and uneducated rants about technology are only making them look much worse.

Thomas ends her op-ed by writing: "Connected technology has the potential to revolutionise our cities for the better, and we should fully embrace that potential. We just have to be smart about it."

Sure. I would add, "Attacking companies for this, that and the other is perfectly kosher. One just has to get one's facts right."

Sam Varghese

US CHIP COMPANIES SEEK TO EASE BAN ON HUAWEI: REPORT

Faced with massive negative revenue impacts, US semiconductor companies are lobbying the US Government to ease the ban on supplying components to Chinese telecommunications equipment vendor Huawei Technologies, a report claims.

Citing "people familiar with the matter", ***Reuters*** **reported** on Monday that Qualcomm and Intel were among the firms trying to get the ban eased, adding that Intel and Xilinx had talked to the Commerce Department in May about the placement of Huawei on the so-called Entity List.

Qualcomm, which is a key mobile components supplier, is a clear leader in the supply of modem chips for the burgeoning 5G mobile handsets market and also an exceptionally strong player in the mobile handsets processors market.

Faced with being severely disadvantaged in the 5G space for its iPhone range, Apple was forced to settle in April with Qualcomm and agree to pay licensing fees for the next six years after a protracted legal battle.

The report comes in the wake of another firm in the sector, Broadcom, **saying last week** that it expected to take a hit of US$2 billion in its full-year revenue due to the ban.

Huawei spent about US$70 billion on components worldwide in 2018 and about US$11 billion of that was spent with US companies, the report said.

The US Government **placed** Huawei and 68 of its affiliates on its Entity List on 16 May, meaning that the company would have to seek permission to purchase any American components it needed to manufacture its products.

Four days later, Google **announced** it was cutting off Huawei's access to future updates of Google's Android and Google Play Store.

On 21 May, the US Commerce Department **eased** some of the restrictions until August, allowing Huawei to maintain and update existing networks and handsets.

Sam Varghese and Stan Beer

TWO BENDIGO MEN CHARGED OVER DOS OF POLICE PHONE LINES

Two men from Bendigo, aged 27 and 28, have been charged by the Australian Federal Police and Victoria Police in connection with automated denial-of-service attacks on police phone lines in October last year.

Police from both organisations searched three premises in Bendigo on Saturday in connection with the warrants served on the two, **a statement** from Victoria Police said.

The 28-year-old is alleged to have been the ringleader and has been charged with:

- "Unauthorised access to data held in a computer, contrary to section 477.1 of the Criminal Code 1995 (Cth.) and punishable by up to 10 years imprisonment;
- "Using a carriage service to make a threat to cause serious harm, contrary to section 474.15(2) of the Criminal Code 1995 (Cth.) and punishable by up to seven years imprisonment;
- "Using a carriage service to menace, harass or cause offence, contrary to section 474.17 of the Criminal Code 1995 (Cth.) and punishable by up to three years;
- "Dishonestly obtaining or dealing with personal financial information, contrary to section 480.4 of the Criminal Code 1995 (Cth.) and punishable by up to five years imprisonment; and
- "Sabotage, contrary to section 247K of the Crimes Act 1958 (Vic) and punishable by up to 25 years imprisonment."

He was jailed and is to face the Bendigo Magistrates Court on Monday.

The 27-year-old was hit with three firearms offences, with the police alleging that he had been in possession of an unregistered firearm in violation of section 6A of the Firearms Act 1996.

He was granted bail and will face court on 8 August.

Chris Goldsmid, AFP acting commander, Cyber Crime Operations, said: "Each occasion a police phone line was unavailable as result of these malicious attacks meant members of the public were unable to access a vital service. This had serious implications for the broader community.

“Some of the attacks included a spate of text messages asking for emergency assistance. People who called the number back reported being verbally abused by a recording on the other end. This created fear, distress and anxiety amongst some of the most vulnerable in our community."

Sam Varghese