CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Monday 22 October 2018

ACMA HANDS TELSTRA A TRIPLE ZERO CANING

CommsWire (ISSN 2202-4549) is published by iTWire Pty Ltd. 907/151 City Rd, Southbank, Vic, 3006
CommsWire/Telecommunications Editor: Stan Beer
Staff writers: Peter Dinham, Alex Zaharov-Reutt, Sam Varghese. Columnist: John de Ridder
Advertising: Director of Digital Media, Andrew Matler: andrew.matler@itwire.com • Tel: 0412 390 000

ACMA PROBE OF TRIPLE ZERO FAILURE FINDS TELSTRA IN BREACH

An ACMA investigation into the lack of provision of a triple-zero service by Telstra after an outage in May has found the telco in breach of a rule that requires it to ensure that such calls go to the emergency call service operator.

The Australian Communications and Media Authority said in **a statement** on Monday that Telstra had failed to ensure some 1433 calls went through to the operator due to **problems** triggered by a fire in an inter-state cable pit. This was compounded by network software failure.

Telstra has to comply with the Telecommunications (Emergency Call Service) Determination 2009 and the Emergency Call Service Requirements Industry Code C526:2011.

Communications Minister Mitch Fifield said a report released by his department into this incident and **one other**, when a large volume of calls were directed to triple zero from the Vocus network, had resulted in 11 recommendations seven of which apply to Telstra.

“The government takes the safety of Australians seriously and the triple zero service is vital in keeping our community safe,” he said.

“This was the first serious disruption to the triple zero service in more than 50 years. With the measures the government is putting in place, Australians can feel confident the service will have greater safeguards in times of need.”

The ACMA said it had accepted a court enforceable undertaking from Telstra in which it committed to improving the redundancy and diversity of its network, developing new communication protocols to be used in the event of another disruption and benchmarking its systems against international best practice.

"Triple zero is the lifeline for Australians in life-threatening or emergency situations. Community confidence in the emergency call service must be maintained," said ACMA chair Nerida O’Loughlin.

"The actions Telstra has already taken, and is undertaking, will help strengthen the emergency call service and minimise the risk of another disruption to this critical service."

The ACMA said it was also reviewing rules governing the emergency call service to ensure they were as robust as possible and that they imposed clear, consistent and appropriate obligations.

"Given the critical nature of the Triple Zero service, the ACMA takes matters about access to the service very seriously," O'Loughlin said.

"The review will help ensure that the rules for the emergency call service remain current and effective."

Sam Varghese

ENCRYPTION: CONSULTATION? WHAT CONSULTATION, ASKS CA

Communications Alliance chief John Stanton has questioned the Federal Government's claims about having consulted widely before drafting its encryption bill, saying he had just a single meeting with the attorney-general's office prior to release of the public draft.

The **Parliamentary Joint Committee on Intelligence and Security** held the first day of hearings into what is officially known as the **Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018** on Friday.

Stanton contrasted the degree of consultation he had been accorded over this bill with that which the CA had experienced during the drafting of the **Telecommunications Sector Security Reforms** bill.

He said he had been consulted thrice during various stages of drafting to ensure that industry was satisfied with what was finally enshrined in legislation.

Also taking aim at the level of consultation, which Hamish Hansford of the Department of Home Affairs claimed earlier had been "wide-ranging", was Dr Suelette Dreyfus, who appeared at the hearing representing rights body Blueprint for Free Speech.

Dr Dreyfus, who is a well-known and respected technology researcher, said the consultation that had been gone through was not representative of a democracy, only a "faux democracy".

The hearing featured a packed agenda, making it impossible for those who appeared to have more than a small bite of the cherry: appearing on a day which ran to less than eight hours were representatives of the following organisations:

- ASIO
- the Department of Home Affairs
- the AFP
- the Australian Signals Directorate
- the Australian Criminal Intelligence Commission
- the Australian Border Force
- the Law Council of Australia
- Telstra
- Optus
- Cisco
- Communications Alliance
- the Australian Industry Group
- the Australian Information Industry Association
- the Australian Mobile Telecommunications Association
- BSA | The Software Alliance
- Electronic Frontiers Australia
- Blueprint for Free Speech
- Digital Rights Watch
- Future Wise and
- Access Now.

Cisco was well represented, with four staff, including Eric Wenger, director, Cyber Security and Privacy Policy, Global Government Affairs, and Tim Fawcett, head of Government Affairs, Cisco Systems Australia. Wenger appeared from Washington via a video hook-up, despite the late hour.

The company has good reason to be worried about the bill for it has seen what can happen when the fact that **backdoors have been implemented in hardware** becomes known.

In 2014, it was **revealed** by NSA whistle-blower Edward Snowden that the agency's Tailored Access Operations Unit had back-doored the firmware of Cisco equipment without the company's knowledge, while it was en route to organisations that had been targeted for surveillance.

According to the British newspaper ***The Independent*** at the time: "An analysis of financial filings from technology giants IBM and Cisco by The Independent on Sunday reveals the two businesses have seen sales slump by more than $1.7 billion (£1.03 billion) year-on-year in the important Asia-Pacific region since [Edward] Snowden revealed in June [2013] that US companies had been compromised by the NSA's intelligence-gathering in the clandestine Prism programme."

Wenger suggested that companies be able to mount a court challenge to any decyrption notices they received under the bill.

The organisations and companies that appeared had already advanced their arguments for and against the bill in submissions either made directly to Home Affairs or else to the hearing.

The impact that the bill would have on Australian businesses was highlighted by the CA's Christiane Gillespie-Jones when she pointed out that the equivalent of what Australia had done to Chinese telecommunications firms Huawei and ZTE — banned them from having a role in the 5G rollout — could well happen to Australian IT firms who did business overseas if the bill were passed in its current form.

PJCIS chair Andrew Hastie made light of this assertion, by saying that Australia is not a Communist country.

Perhaps the person who felt most short-changed at the end of the day was Darryn Lim, who appeared for BSA | The Software Alliance, and had flown in from Singapore to appear at the hearing.

Lim, who gave **a detailed interview** to ***iTWire*** last month about the flaws in the bill, represents the views of Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Baseplan Software, Bentley Systems, Box, CA Technologies, Cad Pacific/Power Space, Cad Pacific, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Mathworks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, and Workday.

Hastie said Apple, Amazon and Microsoft had informed the hearing that their views were not being presented by the BSA.

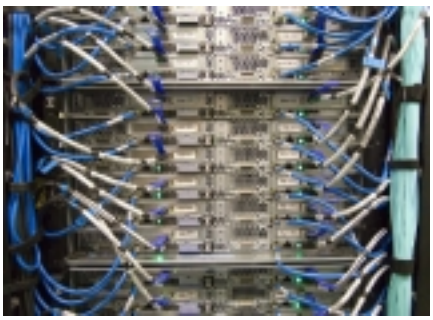
Lim was originally scheduled to have an hour and 15 minutes to present his views and answer questions. But on Friday, he had just 20-odd minutes to make his case and defend it.

Sam Varghese

BANKWEST'S DEBT 'ENFORCEMENT DEFAULT' SLAMMED BY NEXTDC

Bankwest, a division of the Commonwealth Bank, has been accused of launching an "aggressive and overhanded enforcement default" in the case of Asia Pacific Data Centre, by the head of data centre operator NextDC, Craig Scroggie.

The bank demanded a payment of $29 million from APDC, which NextDC is in the process of acquiring, even though it had already agreed to the takeover in late 2017, Scroggie told ***CommsWire***. NextDC itself is worth more than $2 billion.



Bankwest's demand was **first reported** by Fairfax Media on Friday.

"We have certainly seen our fair share of appalling bank behaviour over the years as we have built the company from a start-up to over $2 billion, but our most recent experience with Bankwest is worthy of note," he said.

Bankwest's move came ahead of an APDC promise to pay shareholders a a special distribution of $0.02 per security on 14 November.

NextDC acquired the 67.3% APDC holding of property fund manager Tony Pitt's 360 Capital Group recently for $154.8 million. With that, NextDC owns about 98% of APDC and will gain control on 22 November.

APDC owes Bankwest the $29 million, but it has assets worth $261 million, Scroggie pointed out. Despite being backed by a superior credit party in NextDC, Bankwest still insisted on launching enforcement action against APDC, including sending NextDC a threatening legal letter in its capacity as a tenant to APDC.

When NextDC asked CBA to find out why the debt default notice had been sent, it was told that the query was being passed on to Bankwest.

"The initial response we get from the CEO of Bankwest is words to the effect of 'oh it's not our fault we are just protecting ourselves'," Scroggie said, adding, "Are you serious?"

"Anyone would agree the self-policing of banks has been a laughable failure – they have learnt nothing," he commented. "They espouse value statements like 'Our customers are at the heart of everything we do'… 'We take ownership'. As the 1.5-star online customer reviews of Bankwest suggests, the customers beg to differ!"

CommsWire contacted Commonwealth Bank for its take on the issue. A spokesperson for Bankwest said it would be inappropriate to comment at this stage as discussions between the parties involved were continuing.

Sam Varghese

OVER THE WIRE TO ACQUIRE ACCESS DIGITAL NETWORKS, COMLINX

ASX-listed telecommunications, cloud and IT provider Over the Wire has inked binding agreements to acquire all the shares in Access Digital Networks, and all shares in Comlinx.

The deal sees Access Digital Networks being purchased for $10.4 million and Comlinx bought for $12.8 million.

The acquisitions by **Over the Wire** are fully funded by an institutional placement of $21.5 million priced at $4.30 per share and existing cash, with completion of the acquisitions expected by the beginning of November.

Access Digital Networks is a South Australia-based provider of business grade telecommunications services.

Brisbane-based Comlinx is a provider of IT managed solutions offering cross-sell opportunities to the Over the Wire group.

Over the Wire says the acquisitions are a continuation of its existing business strategy and will contribute to group earnings from 1 November.

The company also says the acquisition of Access Digital Networks accelerates its geographic expansion into South Australia.

The acquisition of Comlinx provides its customers with a broader product offering and additional value added services that can facilitate the pull through of revenue from its network and voice divisions.

Over the Wire managing director Michael Omeros said, “We are very excited to be able to welcome Access Digital Networks and Comlinx to the Over the Wire group. Access Digital Networks and Comlinx are high quality businesses with quality teams that will integrate well with Over the Wire.

“Access Digital Networks expedites our geographic expansion plans into South Australia whilst Comlinx introduces some complimentary new offerings via intelligent networks, contact centre / customer experience and cyber security solutions, which will be of great benefit to our existing customers.

“We will continue to target 20% year on year organic growth, together with achieving very high levels of customer retention."

Peter Dinham

TIM COOK CALLS ON BLOOMBERG TO RETRACT CHINA SPYING STORY

Apple boss Tim Cook has asked Bloomberg to retract a story it published earlier this month, claiming that his firm was among companies that were exposed to spying through chips implanted on server mainboards made by US company Supermicro Computer.

Cook **told** ***Buzzfeed News*** in a phone interview: "There is no truth in their story about Apple. They need to do that right thing and retract it."

Apple issued a detailed denial when the **story** was published. Later, its former general counsel, Bruce Sewell, **said** that the FBI had told him it had told him it had no knowledge of any probe into such an incident, as claimed by Bloomberg.

And the company took the additional step of **writing to the US Congress** denying the story. Chief security officer George Stathakopoulos said in **a letter** that the company had found no evidence to justify the claims made in the ***Bloomberg*** report.

In **its story**, ***Bloomberg*** claimed security testing by Amazon in 2015 had revealed the existence of tiny chips that were not part of the original mainboard design and that this led to an extensive investigation by US Government agencies which found servers built using these boards in data centres belonging to the Department of Defence, on warships, and for processing data being handled by CIA drones.

The news agency said that major banks were also using servers made by Supermicro and that the government investigation led to several companies getting rid of the equipment.

A few years ago, Robertson and Riley put out a story, claiming that the US Government had prior knowledge of the Heartbleed bug, a serious vulnerability in OpenSSL, before it was announced. Bloomberg did not issue a follow-up after the story **was denied**.

Cook said: “I was involved in our response to this story from the beginning. I personally talked to the Bloomberg reporters along with Bruce Sewell, who was then our general counsel. We were very clear with them that this did not happen, and answered all their questions. Each time they brought this up to us, the story changed, and each time we investigated we found nothing.”

He said the likelihood of an incident like the one Bloomberg claimed could happen without him knowing about it, had odds that were more or less zero.

“We turned the company upside down. Email searches, data centre records, financial records, shipment records. We really forensically whipped through the company to dig very deep and each time we came back to the same conclusion: This did not happen. There’s no truth to this.”

Bloomberg told ***Buzzfeed*** that it stood by its story.

Sam Varghese