

THE AUSTRALIAN

Family Planning's epic security fail

MICHAEL CONNORY THE AUSTRALIAN 9:23AM May 21, 2018

It seems ANZAC Day 2018 will be remembered by 8000 New South Wales women as more than just Australia's National Day of mourning to honour the sacrifice of the fallen in conflicts of theatre Australia has been engaged in.

For them, April 25, will have an equally different side to it. It will be remembered as the day, Family Planning NSW, failed to protect their privacy and health details.

ANZAC Day shouldn't be thought of as a day when hackers were able to crack through Family Planning NSW's security, it has greater prominence of elevation in our minds, but for 8000 women, it will have a different meaning now.

As big as crises can get, this is epic, and Family Planning NSW are failing to acknowledge the enormity of the issue. It smacks of poor governance and not taking the time and effort to protect the information of clientele it's meant to protect.

Circulating for some time, in the grip of hackers, was highly sensitive information on vulnerable women, and yet, Family Planning NSW CEO Ann Brassil declared records and data stored internally were ok. This is an odd form of rationalisation, especially when hackers were able to breach the Department's security.

In the midst of the breach, the acceptance by NSW's Family Planning hierarchy to do anything other than create white noise and tenuously work to correct the problem and restore the confidence of women affected is a breach of trust.

Instead, a simple email was sent out - no detailed explanation, no remediation, no reassurance to advise of reviews and tighter controls and applications being put in place to ensure the problem will never be repeated, just a letter of minimal detail. The minimum required by law.

Breaches of any kind are serious, and it goes straight to the heart of questioning whether it has or had the appropriate technological infrastructure and capability to protect its client's information.

It's now obvious, it didn't, and Ann Brassil, through her comments, were clear, she was failing to recognise a hacker having access to the names and contact details of the impacted women was a significant risk - imagine the consequences to the women if information were released.

Marvelling from the side lines of what can only be described as a disaster, Family Planning NSW continues to not address the issues of concern that haven't been addressed so far.

Issues it needs to focus on that help to repair its reputation and put in place robust strategies for the future, ensuring it is able to deal confidently with speed to guard against any future breaches.

Investment in technology and how it works to guard the safety of information is critical. But to allow those issues to fester and not address the key elements of the problems as were presented on ANZAC Day, is a failure of trust, especially when it knew it had a system vulnerable to attack.

Family Planning NSW needs to address key concerns I believe it hasn't. Concerns around: Why didn't it conduct a thorough screening of third-party providers - especially after the Blood Service breach of 2017?

- How it is a third-party supplier, Adelphi Digital Consulting Group allowed itself to be vulnerable to the Drupalgeddon 2. Drupalgeddon 2 allows any person on the net to take control of vulnerable servers, like Adelphi's by accessing a URL and injecting an easily accessible exploit code.

Addressing issues immediately allows to mitigate outcomes damaging to all affected, and from what is now known, Family Planning NSW failed to act on its vulnerability to attack well before April 25, when it knew in March, it had a problem.

Warnings on this specific attack, to the servers managed by Adelphi, had been issued early April - yet like many organisations, it failed to act.

Of further interest is NSW's Minister for Health, Brad Hazzard's, statements around health funded NGOs having to comply with privacy and data standards.

It shows a level of naivety around an issue given the world we know live in of a lack of understanding of what needs to be achieved to safeguard privacy – saying health funded NGO's need to comply with privacy and data standards, doesn't mean they are not vulnerable to attack.

Family Planning NSW's breach raises other questions of concern around how well protected every Australian's personal data and information is with other health providers as well as government agencies? Today people have begun opting out of the Federal Government's My Health Record as fear about data security grows.

The time has now come for mandatory third-party supplier security audits to be conducted.

If simply nothing has been learned from ANZAC Day 2018, then like the perils of conflict, peace cannot be had if the marches and parades aren't a glaring reminder of what was sacrificed.

Unfortunately, the lessons of April 25, 2018, have to be learned by all corporations to protect the sensitive information and privacy of their clients.

But don't head to Family Planning NSW's web just yet for further information, the site still remains down.

Michael Connory is the Founder and CEO of Security In depth.



MARGIN CALL

Culleton keeps inquiry on track

WILL GLASGOW, CHRISTINE LACY

Farmer turned senator turned self-taught constitutional scholar Rod Culleron was the star attendee at the Hayne Show today.



COMMENT

AGL weighs political discomfort

ANDREW WHITE

By rejecting an offer for Liddell, AGL must calculate it's worth more than the political pain it's enduring, from the PM down.



Jones relied on 'eyewitness stories'

MARK SCHLIEBS

Alan Jones had 'eyewitness' accounts but no scientific evidence when he linked a quarry to the deadly 2011 Grantham floods.



DATAROOM

Afterpay founders offload shares

BRIDGET CARTER

Afterpay founders Anthony Eisen and David Hancock are selling shares in the company in a block trade executed by Citi.



Yuhu unveils \$3bn property plan

LISA ALLEN, BEN WILMOT

Yuhu Group has revealed plans to sink \$3bn into updating the Sydney and Gold Coast projects it acquired off Wanda.



EXCLUSIVE

Old-age super products a 'fraud'

MICHAEL RODDAN

New super income products designed to encourage spending in retirement have been slammed as 'actuarial fraud'.

A NOTE ABOUT RELEVANT ADVERTISING: We collect information about the content (including ads) you use across this site and use it to make both advertising and content more relevant to you on our network and other sites. This is also known as Online Behavioural Advertising. You can [find out more about our policy and your choices, including how to opt-out here](#)

[^ Back to top](#)



The Australian app

Our Products

- The Australian app on iOS
- The Australian app on Android
- Facebook messenger app
- Chinese Site
- Today's paper

Terms of Use

- Editorial Code of conduct
- Standards of Practice
- Subscription terms
- Group Subscription Terms
- Accessibility
- Privacy Policy
- Relevant Ads Opt-out
- Cookie Policy

Contact Us

- Help
- Contact Us info
- Photo Sales
- News Archive

About Us

- About The Australian
- Advertise with us
- Our journalists
- Subscribe
- The Australian Plus member benefits
- Sign up to Newsletters
- Manage Your Newsletters

Copyright The Australian. All times AEST (GMT +10:00)