THE AUSTRALIAN

Cybersecurity ‘policy’ in chaos

MICHAEL CONNORY

By **MICHAEL CONNORY**
12:00AM JULY 2, 2019 • 2 COMMENTS

Cybersecurity incidents in Australia are out of control and we find ourselves compromised with no real plans to address the issue.

Lack of funds, a fly-by-the-seat-of-the-pants attitude and a naive understanding that confuses cybersecurity as an IT problem have put us in an unenviable position. Organisations know they need to take measures but are struggling to turn words into meaningful action. Everyone seemingly has a plan; that is, until sensitive data is leaked and boardrooms hit the panic button.

The anointed cop on the beat, the Office of the Australian Information Commissioner, is largely limited in its enforcement capabilities, hamstrung by a criminal lack of resources. All the while, the volume of cyberattacks keeps rising. Cyber breach notifications have increased 712 per cent since 2018 and actual attacks are up 2000 per cent.

This year, Parliament House was breached, PageUp hacked, the Australian National University came clean on another major attack and the banks continue to prove easy pickings, with Westpac recently facing a serious breach. While breaches continue, we have not heard from government on what is being done to protect our information.

Cybersecurity should have been a policy battleground tackled by both sides of politics during the election, but wasn’t — and that was disappointing.

Australians justifiably should feel let down by the lack of commitment from both parties to tackle the issue with the same level of intensity shown on giving law enforcement agencies more power to police the internet.

The so-called Telecommunications and Other Legislation Amendment (Assistance and - Access) Act 2018, which allows agencies to pry open encrypted messages, was waved through despite strident criticism in the name of national security.

Yet the same vigour seems to be sorely lacking when it comes to cybersecurity. We now live in a world where everything we do is data-dictated; however, we have few plans drawn up to safeguard everyday Australians. Our strategic war chest is bare.

Scott Morrison is a hardened politician and after pulling off a spectacular political victory, he has a chance to bed down a fundamental, legacy-building measure on cybersecurity. In a world where digital threats can undermine the safety and security of citizens, the Prime Minister must appoint a minister dedicated solely to cybersecurity.

The government's promise to commit $156 million for cybersecurity is a drop in the ocean, given what's required to protect our vital assets and bring us in line with the rest of the world.

We haven't had a cybersecurity minister since Malcolm Turnbull was ousted. Leadership in this area is critical but we remain rudderless; having cybersecurity fall under Homeland Security and Peter Dutton is nonsensical.

Our safety and security is far less at threat at our physical borders and from boatpeople seeking refuge from persecution. It's the virtual borders where the true dangers lurk in the shadows.

However, cybersecurity isn't just a technology problem; it's a people problem, it's a behaviour problem and it's about culture.

A lot of that stems from our lack of regulation and legislation.

Couple that with an ongoing shortage of cyber skills and there has never been a better time for the government to grab the cybersecurity bull by the horns.

Michael Connory is chief executive of Security in Depth.