




Speech By
Hon. Leeanne Enoch

MEMBER FOR ALGERTER

Record of Proceedings, 3 December 2015

MOTION

 **Hon. LM ENOCH** (Algerter—ALP) (Minister for Housing and Public Works and Minister for Science and Innovation) (6.25 pm): I rise to oppose this motion and to make it quite clear that the Queensland government takes any criminal act very seriously. That includes acts of cyber security.

I mention in response to the comments of the member for Mansfield that on 7 June 2013 he tabled the ICT audit in this parliament. He did not table the confidential annex which would have revealed the security risks. He says today that there should be full transparency. Thankfully, he was a little more responsible when he was in government.

When this incident came to the government's attention the immediate and most important actions were to block any further damage and to limit access to the stolen data. The affected systems have been remediated and the data is not publicly available on the internet. We notified federal and state police agencies as well as the Australian Cyber Security Centre. Their investigations are continuing.

The Queensland Government Chief Information Office, QGCIO, was tasked to work with the affected agency on the security breach and what can be done to safeguard its systems from future attacks. Our IT security experts are continuing their forensic analysis. That may take some time given the anonymous nature of this activity. The risk of the perpetrator publicly releasing the data still exists. Control efforts are ongoing to mitigate this risk.

We are taking this matter very seriously. That is why we have accepted the advice of the QGCIO and the police that any public release of further information could impact their ongoing investigation. Unfortunately, the LNP members in this state seem to have little respect when it comes to the responsible way to behave in the face of these types of matters.

This government extended an invitation to members opposite to attend a confidential briefing on this incident. I understand that the member for Everton said that he would attend on behalf of the Leader of the Opposition and the member for Surfers Paradise. I find it deeply concerning that, despite knowing the risks involved, members opposite have flagrantly ignored all advice and continued to pursue this matter in the hope of scoring cheap political points.

Just yesterday in the federal arena we learned about a major cyber attack on the Bureau of Meteorology. ABC News coverage states that the bureau owns one of Australia's largest supercomputers and provides critical information to a host of agencies. It stated—

Its systems straddle the nation, including one link into the Department of Defence at Russell Offices in Canberra. Cyber attacks on government agencies are routine and the 'adversaries' range from thrill-seeking hackers, through to criminals and foreign states.

The ABC report references a spokesperson for Prime Minister Malcolm Turnbull. What did the PM's office have to say in relation to this cyber attack on the weather bureau? In a statement, the Prime Minister's spokesperson said that 'the government would not comment on specific cases'. Perhaps the

Prime Minister can come up to Queensland and give those LNP members opposite a lesson in responsible conduct in the event of a crime being committed against a government system.

IT vulnerability is, unfortunately, a reality for governments and major corporations in the modern age. This is not just a Queensland government issue; this is an issue for major corporations and for governments around the world—for anyone doing business in 2015. In recent months we have heard reports of the biggest hack in United States history, with the fingerprints of 5.6 million current and former government officials stolen. The United States largest bank JP Morgan is among the growing list of major corporations who have had information stolen, and we know that identity fraudsters now regularly target Australian tax records.

A number of high-profile examples of cybersecurity incidents have been covered in the media in recent days, such as those experienced by Aussie Farmers Direct, cloud based accounting companies, the federal government, Kmart and David Jones. This type of attack is increasing in both its sophistication and its frequency, and it is nothing short of criminal. The QGCIO is observing an elevated level of cybersecurity incident activity across the public sector and it is concerning that many of the incidents appear to be criminally based.

No-one can afford to be complacent and I want to assure Queenslanders that the government is committed to fully investigating and remedying this breach. I am committed to efforts to safeguard the government's network from further attack and can advise that the government has put in place further IT measures to protect and strengthen our security protocols and systems.

In relation to the second part of the member's motion, I would be happy to provide the Utilities, Science and Innovation Committee with an in-camera update on investigations into this matter when I brief the committee on 17 February 2016.