CYBERSECURITY

Statement

HON WILSON TUCKER (Mining and Pastoral) [6.22 pm]: In the dying embers of this year, I thought I would give members another update on everyone's favourite topic—cybersecurity. I have mentioned previously that I recently spoke at a conference in Dubai on cyber resilience in the resources sector. I went on a bit of a journey, speaking to stakeholders in the cyber space in Western Australia and Canberra. I came away with a few interesting factoids that I thought I would share with members. I will see how I go in 10 minutes.

Firstly, when we talk about cybersecurity, we need to acknowledge data security and the importance of data. For a long time in Australia, companies would not understand the importance of data. They certainly understood it from a monetary or corporate perspective, but not from a risk or compliance perspective. A lot of companies have a lot of information in spreadsheets and databases that they sometimes need, but as the footprint of that information increases, they also need to make sure that they are taking adequate steps to protect it. Members will be aware of the large number of data breaches that we experienced last year, and I have spoken about this previously. Optus, a telecommunications provider; Medibank, a medical insurance provider; and Latitude Financial Services, a financial services company, were hacked. About 20 million records of highly sensitive and confidential personal and medical information was leaked onto the dark web and then sold to the highest bidder. Given that there are 25 million Australians, it affected the majority of the population, including our Prime Minister.

This has really put cybersecurity at the top of the federal government's agenda. It has recently reviewed its cybersecurity strategy. It also put through the Privacy Legislation Amendment (Enforcement and Other Measures) Bill last year, which increased the penalty for companies that are asleep at the wheel and not doing enough to protect information. The penalty went from $2.2 million to $50 million. A penalty of $2.2 million would not give some companies too much pause for thought, especially tier 1 miners, but a penalty of $50 million kind of would. Beyond the financial penalty, the reputational damage can be a lot more severe. Unfortunately, when we talk about resource companies and cybersecurity, we find there is an apathy by boards and CEOs about cybersecurity. A recent report by BDO showed that a lack of emphasis or importance was placed on cybersecurity by resources sector boards; meanwhile, the number of cyber attacks in the resources sector was actually quadrupling. There was a disconnect between what boards deemed important and what was actually happening in the real world.

The other point I will raise is the supply chain—what industries can do to ensure that their supply chains are protected. Tier 1 miners should have the resources to ensure that they are keeping pace with any regulatory requirements in the cyber space and that they have the expertise to keep updated with a threat landscape that changes very quickly. However, a deficit or a gap exists at the moment with the tier 2 and 3 miners and the suppliers of the tier 1 miners.

The federal government recently changed its critical infrastructure act. Four industries were deemed as critical infrastructure industries, and the industries that are considered to be critical have to go through added compliance. They have to communicate with the Australian Signals Directorate, which is basically our National Security Agency or our cybersecurity agency. They have to alert the ASD if there is an incident. They also have to give it reporting information to ensure that it has a holistic view of what is going on to understand any patterns in attack vectors and that it can communicate that to industries if required. Now there are 11 industries. Ports are considered critical, as are the energy production and petroleum industries. Oil and gas businesses are considered critical, but iron ore businesses are not. It has sort of split the resources sector in two. If a company has a breach, it has to work alongside the ASD.

There is also a thing called the critical infrastructure uplift program. That is being run out of the Australian Cyber Security Centre based in Perth. Its remit is to try to uplift industries to make them aware of what is going on and ensure that they have the expertise to respond to cyber attacks. It is all well and good if an industry is considered critical, but the miners that are not, especially the tier 2 and 3 miners and their suppliers and dependencies in the supply chain, do not have access to those resources, so there is still a deficit there. All levels of government—not just the federal government, but state governments as well—have a responsibility in running this program to ensure that the entire supply chain is protected. That is really a top-down approach to raising the awareness of cybersecurity within an industry. It is also important to adopt a bottom-up approach that is industry led to ensure that an industry's dependencies are still working. Much in the same way that companies will pass down their environmental, social and governance requirements to their suppliers in terms of scope 2 and scope 3, larger companies especially should be having that conversation with their dependencies within the supply chain to make sure that they are not vulnerable and affecting the business essentially at the same time.

I will share with members a recent story about a tier 1 miner. I cannot remember which one, but I believe it was in the Pilbara, so members could probably guess it pretty quickly. It had a contract with a motel to house its FIFO staff. The motel was a small business; I think it was a mum-and-pop shop operating out of the Pilbara. It was constantly getting attacked and its information breached. All the employee information from this tier 1 miner

was being accessed. This tier 1 miner found out about it and told the business that if it continued to happen, it was going to sever ties and cancel the contract because it was compromising the information of the miner's employees. These people were in the business of running a hotel but did not have the expertise to manage their IT infrastructure. They got hacked again and the tier 1 miner cancelled the contract as a result. I believe it was quite detrimental to that business.

There is a gap. If the government is not going to fill that gap, there certainly needs to be an industry-led initiative, but state government has a role to play. If one corporation, company or entity is being attacked, it might be slightly beneficial for a company to compete on cybersecurity, in a sense. The other competitor has not suffered any reputational damage as a result, so they might see a short-term windfall, but it really sets a target on the back of the industry as a whole. Although it is not good in the long term, some companies might see it benefiting them in the long term.

I will jump ahead in my remaining minute. What are the major challenges for government? One of the big challenges right now is a lack of trust in governments. We have seen that with the Australian Signals Directorate releasing a report that shows an underreporting of cybersecurity incidents. The main reason that companies were not reporting is because they did not trust that the government, when provided with that information, would use it only for the purposes of a cybersecurity incident. The companies thought that the information could be used against them as part of a future litigation case or that it would go into this black box of government to be shared around a lot of different agencies. In response, the federal government is putting in place some ring-fencing legislation to ensure that when information is provided as part of a cybersecurity incident, it is used for only that purpose.

I will give members a quick takeaway as we head into the Christmas break. When we talk about data sharing and privacy, it is important to get the legislation right. Western Australia still does not have any data privacy legislation that governs the public sector. It makes it more difficult for agencies and certainly the private sector to share information within the four walls of the public sector. I have a little more to say. I have run out of time but I will continue harping on about it in 2024.