CYBER ATTACKS

Statement

HON WILSON TUCKER (Mining and Pastoral) [6.25 pm]: I would like to give members a brief update on the current state of cyber and the risks posed to the WA resources sector. We know that the resources sector in WA is the engine room of the economy and it is very important we keep it ticking along. The cost to the Australian economy through cyber attacks is around 1.9 per cent of our GDP, which is equivalent to about $29 billion a year. That number is expected to grow exponentially. It is obviously a massive figure. It has overtaken the illicit drug trade. It is more beneficial for criminals to steal our data than it is to sell us drugs. As well as the financial implications to the Australian economy, the WA economy and businesses and entities, there is also the reputational damage, which in some cases is more significant than the financial burden. Optus and Medibank are clear examples of that; the companies really took a reputational hit and are still dealing with the fallout.

There are a few truisms in the cyber space. One is "It is not if but when" and the other one is "There are those who have been breached and those who do not yet know they have been breached." Both these really speak to a mindset that needs to be adopted by entities and companies when it comes to cyber. Companies never really truly reach a state of nirvana around cybersecurity. A system is never 100 per cent safe. It is a moving target and the landscape moves very quickly. That is why reports by the Attorney General that really highlight the state of the IT infrastructure for state government entities are really important, because vulnerabilities have been identified in one of the annual reports. There is a flow-on effect and a rollover with a high percentage of those still present the next year, which is obviously concerning to me and to the Attorney General. It is a sector in which changes are measured in hours and days. They are not measured in weeks or months and certainly not years.

Plenty of tools are available on the dark web for hackers and the landscape really changes quickly as the attack vectors for hackers evolve as well. As businesses and entities move online and embrace the digital economy and the digitisation of services, it presents more opportunities for people to access the system and steal people's data. Also, as systems become obsolete, there is a growing need to really pay back that tech debt and make sure that systems are up to date. The analogy is a moving target as opposed to a stationary one. If we do not install those firmware and software updates, the system does not have those security patches and is basically a stationary target and it is very easy for hackers to find vulnerabilities and exploit them. It is really a mindset that has to be instilled within the organisation. It cannot just lie with the manager. It has to come from the CEO and the board level—a top-down directive instilling a culture of cybersecurity awareness within an organisation.

Members will be aware of a recent cybersecurity attack on DP World, which affected operations in the major Australian ports of Sydney, Melbourne, Brisbane and Fremantle. I believe that about 30 000 shipping containers were piled up at one of the terminals, which affected operations for a number of days. That attack has been resolved. An investigation into how it happened and who was responsible is still ongoing. The Australian Federal Police is investigating, along with the Australian Cyber Security Centre, which is based here in Perth. I believe that the Australian Signals Directorate is also involved.

The Cyber Security Centre works with businesses and makes them aware of any compliance coming from federal legislation in response to cybersecurity. The Australian Signals Directorate, Australia's cybersecurity intelligence agency, released a report yesterday on the current state of cybersecurity as it sees it. It is the authority on cybersecurity in Australia. Some of the statistics are actually quite damning. The average cost of cybercrime is up 14 per cent. On average, it costs a business $71 000 when it is attacked. Nearly 94 000 cybercrimes were reported in the last financial year, which is up 23 per cent. On average, a report was made every six minutes. It received over 33 000 calls during that year. The top three cybercrimes for individuals are identity fraud, online banking fraud and online shopping fraud. The top three cybercrimes for businesses are email compromise, business email compromise and online banking fraud.

Typically, attacks are monetary in nature. A classic example is someone who gains access to a person's system, saying, "Give us a couple of million bucks in bitcoin or crypto and we won't leak your dataset or your clients' personal information on the dark web", or they could basically install some ransomware, getting into their system, locking it down and disrupting their business until they pay that ransom, when they restore access back into the system.

The more troubling scenario and one that we are seeing increasingly is sophisticated state-backed hackers who want to disrupt supply chains, gain a market advantage or cause havoc for other geopolitical reasons. The Optus hack was attributed to Chinese-backed hackers, which probably helps with the reputational damage for Optus a little as we can all point to a foreign entity and say that it was responsible. The reality is that despite the fact that the hackers were very sophisticated, the hack itself was not. It involved an API endpoint, a development endpoint, linked to a production database. It was set up for ease of access for developers' testing. A quick penetration test would have picked this up. The blast radius was obviously huge, with millions of Australians' information leaked.

I wish to talk about the resources sector in particular in the minutes that remain. We know that WA has a lot of experience in remote operations capabilities. During the COVID-19 pandemic, miners really tried to automate their operations. The Venn diagram between operational technology and the ability to automate the operations of their equipment and machinery onsite and their IT systems that hold all their operation is merging. Their footprint is expanding. A recent report by PricewaterhouseCoopers found increased apathy at the board level within Australian companies, not just in the resources sector but across the board. When we talk about an increase in the digital footprint, more attack factors for hackers and then an apathy at the board level, which trickles down through the organisation, that is obviously a concern.

As bad as the attack on DP World was, it affected retailers, potentially people selling goods and maybe getting Christmas presents. I believe that the operation at Port Hedland is the largest bulk export port in the world and the second largest iron ore port in the world.

Hon Dan Caddy: By volume, largest.

Hon WILSON TUCKER: Perhaps the Leader of the Opposition can do the napkin maths, but if we shut down the port for a number of days, it would be pretty easy to calculate the cost to Australian gross domestic product and to the WA economy. It would be significant. If we think shutting down a port for a couple of days is a thing of fiction, the Israelis did it to an Iranian port back in 2020 for four days. It certainly can be done. We have the critical minerals agreement with the United States and AUKUS. It does present the critical infrastructure in Australia and certainly in WA as becoming a target for state-backed hackers.

I have run out of time. I have more to say on this issue. It is a topic that moves quickly. I will update members in the future.