Submission to the 2023-2030 Australian Cyber Security Strategy discussion paper

By Mark Arena

23 March 2023

Mark Arena is an advisor and board member to fast growing cybersecurity startups including the US headquartered cybercrime intelligence firm Intel 471 and drone threat intelligence firm DroneSec. Mark Arena founded Intel 471 in 2014 whilst living in Europe and was the CEO until February 2023. Mark led Intel 471 from its incorporation and through an acquisition by a large US private equity firm in September 2021. Intel 471 works with a number of the world's largest companies and government departments including the Australian Signals Directorate and the Australian Federal Police[1] and has customers across every continent other than Antarctica. Prior to Intel 471, Mark was previously employed by iSIGHT Partners (now a part of Mandiant/Google) to lead global cyber threat intelligence collection activities against sophisticated cyber threat actors and groups in the areas of cyber espionage, financially motivated cybercrime and hacktivism (politically motivated hacking). Prior to iSIGHT Partners, Mark worked for the Australian Federal Police in Canberra as a technical specialist within the High Tech Crime Operations function. Mark has over a decade of experience in proactively tracking and building capabilities against the most sophisticated cyber threat actors across the globe. After living the last decade in Europe, Mark relocated back to Australia in early 2022.

Dear The Expect Advisory Board of the 2023-2030 Australian Cyber Security Strategy,

Thank you for the opportunity to send a response to the 2023-2023 Australian Cyber Security Strategy discussion paper. This submission is based on my experience over the last decade running a fast growing cyber threat intelligence vendor that employs hundreds of people globally and works with the largest and most sophisticated (from an information security perspective) organisations globally. This submission is also based on my experience proactively tracking and building capabilities and investigations against the most sophisticated cyber threat actors globally across my time in government and the commercial sector. In my view and in response to Minister for Home Affairs and Cyber Security Hon Clare O'Neil's goal to make Australia the "most cyber secure country" by 2030, I believe the following goals will need to be achieved:

- Australia accurately understands the impact of cybercrime to Australia;
- Australia becomes demonstrably amongst the best in the cyber protection of its citizens and organisations;
- Australia is regarded by cyber threat actors as a hard target to attack;

---

[1] https://www.tenders.gov.au/Search/CnAdvancedSearch?SearchFrom=CnSearch&Type=Cn&AgencyStatus=-1&Keyword=Intel%20471&KeywordTypeSearch=AllWord&DateType=Closed

- Australia is regarded by cyber threat actors as not worth the pain given the expected response to impacting Australia;
- Australian organisations and their leadership are held accountable for their cyber security posture and improper cyber risk oversight;
- Australia is seen by global companies as the best place in Asia Pacific to establish regional security operating centres (SOCs) and regional headquarters;
- Australia proactively supports the establishment and running of Australian staffed cyber security companies, even if they are formally headquartered in the United States.

Based on these goals, I believe the following recommendations will help Australia meet these goals:

- Australia should commission the Office of the Australian Information Commissioner or another agency to investigate and publicly report on significant breaches of Australian organisations and the lessons learnt from these.
- Australia should commission the Australian Criminal Intelligence Commission (ACIC) or another agency to produce a yearly public report on the impact of cybercrime to Australia.
- Australia shouldn't outlaw ransomware or extortion payments but should introduce mandated reporting of these payments when they are made.
- Australia should examine whether the current multi-agency cybersecurity setup in Australia is fit for purpose and whether it might be time to change the current setup into a single agency[2] with a wide remit.
- Australia's fight against financially motivated cybercrime including ransomware should be expanded to include overt deterrence in addition to apprehension and disruption.
- Australia should adopt a firm stance and legislation with respect to the responsibility of C-Suites and Boards in cyber risk management and make them accountable in a similar way as in the EU (NIS2, DORA) and the US (SEC, NYFS). It should also seek to make the head of Australian government departments accountable for their security posture and breaches within their departments which would set an example of the level of accountability expected from leaders of companies in the private sector.
- Australia should focus on what incentives can be provided to global companies that have a "follow the sun" or 24/7 model to locate regional security operations centres (SOCs) in Australia.
- Australia should look at a range of options to further grow and support Australian staffed cybersecurity companies.
- Australia should look to create a cyber focused investment fund under the Future Fund that emulates Singapore's ISTARI (a subsidiary of Singapore's Temasek sovereign wealth fund) to accelerate global cybersecurity companies building a presence in Australia and to invest in Australian staffed cybersecurity companies.

As a result, I will break up this submission into four main sections:

- Understanding;
- Becoming a hard target and imposing cost;
- Accountability;
- Enabling business.

[2] https://www.theregister.com/2016/11/17/police_civilian_cyber_superagency_australia/

Thank you for your time reading my submission.

Regards

Mark Arena

Understanding

Australia should commission the Office of the Australian Information Commissioner or another agency to investigate and publicly report on significant breaches of Australian organisations and the lessons learnt from these.

In November 2016, Tesco Bank (based in the United Kingdom) was subject to a significant cyber attack. In late 2018, the United Kingdom's Financial Conduct Authority (FCA) released a report[3] into the incident which covered how the attack unfolded as well as deficiencies in the bank and its response which allowed the attack to ultimately be successful. The FCA ultimately fined Tesco Bank £16,400,000 but the report provides sufficient detail of lessons that can be learnt by other organisations to hopefully avoid the same fate. Australian organisations would be better protected against breaches if they were able to understand in detail how a number of recent large breaches of Australian organisations would have occurred.

Australia should commission the Australian Criminal Intelligence Commission (ACIC) or another agency to produce a yearly public report on the impact of cybercrime to Australia.

Whilst public reporting on security breaches in Australia has increased, I believe that most incidents are still not reported. In order to adequately resource the fight against cybercrime, the scale of the problem, which I expect is significantly larger than publicly reported, must be understood. I believe the Australian Criminal Intelligence Commission (ACIC) is the best suited government agency to produce a yearly public report on the impact of cybercrime based on their remit and ability to compel organisations to share information. The ACIC could combine and anonymise the information they receive so the problem as it related to Australia collectively and by sector could be shared publicly. By understanding the problem, we would all be in a better position to resource the response.

Australia shouldn't outlaw ransomware or extortion payments but should introduce mandated reporting of these payments when they are made.

In late 2022, I read articles such as this[4] which indicated that legislation banning ransomware payments in Australia was being considered by the Australian government. Whilst I note that this hasn't occurred yet as of the time of writing, I wanted my opinion on this to be in this submission. If ransomware payments are outlawed in Australia, it will be small and mid size businesses that are most impacted as large and mid size organisations will ultimately still be able to pay ransomware payments via 3rd parties (accounted for/invoiced as "consulting" or something similar) or subsidiaries/other corporate entities in other countries. I understand that paying ransoms ultimately encourages future criminality but in a lot of cases, businesses have no choice but to pay ransoms or potentially go out of business or be significantly impacted. Following up from my previous point, mandatory reporting of these payments with the context and incident information (i.e. Bitcoin wallets receiving the ransom payments) should be mandated. Within the United States, a number of cybercriminals involved with ransomware attacks are sanctioned and it is not believed that the United States Department of the Treasury's Office of Foreign

[3] https://www.fca.org.uk/publication/final-notices/tesco-personal-finance-plc-2018.pdf
[4] https://www.infosecurity-magazine.com/news/australia-considers-ban-ransomware/

Assets Control (OFAC) would seek to fine[5] companies that even send ransomware payments to sanctioned entities if they report it and information around the incident to the relevant authorities.

Australia should examine whether the current multi-agency cybersecurity setup in Australia is fit for purpose and whether it might be time to change the current setup into a single agency[6] with a wide remit.

In February 2023 the Australian federal government announced that they were seeking to establish a Coordinator for Cyber Security with the Home Affairs department. Currently cybersecurity within the Australian department involves a large number of agencies depending on the motivation of the threat actor (financially motivated cybercrime, espionage etc), who is reporting an incident (critical infrastructure, government agency etc), other reasons and it isn't clear who is responsible for what and with duplicative capabilities across different agencies. Before the establishment of the Australian Cybersecurity Center (ACSC) within the Australian Signals Directorate (ASD), I wrote an op-ed[7] that made the case of a single government agency to handle all cybersecurity matters in the Australian government. Cybersecurity is important to everything that we already do and will be even more important over time so I believe that ultimately this is inevitable although the question is whether this happens in the near future or is something that happens in future decades. Regardless of this, a clear responsibility assignment matrix should be developed so that all stakeholders understand which agency has responsibility for what.

[5] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf
[6] https://www.theregister.com/2016/11/17/police_civilian_cyber_superagency_australia/
[7] https://www.theregister.com/2016/11/17/police_civilian_cyber_superagency_australia/

Becoming a hard target and imposing cost

Australia's fight against financially motivated cybercrime including ransomware should be expanded to include overt deterrence in addition to apprehension and disruption.

Whilst I commend the Australian government in supporting and funding offensive operations against financially motivated cybercriminals[8], I note that no actions publicly have resulted that has led to any potential of overt deterrence of cybercriminals impacting Australia. Whilst the Australian Signals Directorate (ASD) is no doubt skilled and experienced in running covert operations quietly and successfully, what is required to deter cybercriminals in protected jurisdictions (i.e. Russia) is overt actions, publicly tied to Australia and/or the Australian government, which penetrate the perceived anonymity of cybercriminals, cost them money and potentially cause them issues in real life. I am not advocating physical action against cybercriminals here but rather publicly exposing their name, address, financial holdings, net worth and whereabouts publicly to other criminals, in their own language. I believe an action such as this, if tied to Australia, could create a deterrent effect on cybercriminals against targeting Australian organisations in future. The United States has attempted similar deterrent action through public indictments of cybercriminals, wanted and reward programs[9] as well as seizure of funds, i.e. Bitcoin wallets through cryptocurrency exchanges.

---

[8] https://www.afr.com/politics/federal/australia-to-hack-the-hackers-behind-medibank-attack-o-neil-20221112-p5bxor

[9] https://www.fbi.gov/wanted/cyber

Accountability

Australia should adopt a firm stance and legislation with respect to the responsibility of C-Suites and Boards in cyber risk management and make them accountable in a similar way as in the EU (NIS2, DORA) and the US (SEC, NYFS). It should also seek to make the head of Australian government departments accountable for their security posture and breaches within their departments which would set an example of the level of accountability expected from leaders of companies in the private sector.

Europe's NIS2 regulation[10] is focused on achieving a high common level of cybersecurity across European Union member states. Specifically it adds serious repercussions for companies including fines for non-compliance and introduces personal liability for "management bodies", such as company boards and executives[11]. Whilst I commend the Australian government for recently introducing higher potential fines on companies for data breaches[12], the Australian government should look at cybersecurity legislation and regulations in Europe and the United States to ensure legislation and regulation in Australia is in sync. Specifically the potential personal liability for board members and executives of companies that are grossly negligent to cyber risks which ultimately leads to significant security incidents should be looked at.

[10] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
[11] https://www.insideprivacy.com/cybersecurity-2/new-eu-cyber-law-nis2-enters-into-force/
[12] https://ministers.ag.gov.au/media-centre/tougher-penalties-serious-data-breaches-22-10-2022

Enabling business

Australia should focus on what incentives can be provided to global companies that have a "follow the sun" or 24/7 model to locate regional security operations centres (SOCs) in Australia.

Australia is recognised as a country that is easy to do business in. Obtaining visas for experienced and skilled foreign employees isn't hard and lots of people globally would relish the opportunity to live in Australia. Saying that, Singapore is seen internationally as the best place currently for large multinational companies looking to create regional security operations centres (SOCs) in Asia-Pacific. This shouldn't be the case and Australia should look at what incentives, i.e. tax credits, can be provided to multinational companies to establish regional SOCs and teams in Australia.

Australia proactively supports the establishment and running of Australian staffed cyber security companies, even if they are formally headquartered in the United States.

Whilst I understand that the Australian government desires for Australia to have "a sovereign and assured capability to counter cyber threats"[13], I believe it will be very difficult to achieve from an Australian-headquartered cybersecurity vendor perspective anytime soon. I also don't know of a single Australian headquartered cybersecurity company that has been successful and at scale internationally. Incorporating a company in the United States, Delaware specifically, is the default thing to do for any technology company seeking to raise funding at the most optimum valuation and terms, sell their products to the largest organisations and ultimately get acquired or sell at the highest valuation possible. I established Intel 471 as a Delaware C corporation in May 2014 and despite not living in the US (I was living in Europe at the time), I was able to set up the company headquartered there and achieve a bank account and other required items quickly and cheaply.

In 2023, setting up a Delaware C corporation remotely and being based totally outside the United States is even easier than before and there are companies[14] focused on just providing this service. There is no requirement to have anyone physically working in the US for a US headquartered company which means that ultimately you could create a company exclusively with staff in Australia that is formally headquartered in the US. This would enable the company to:

- Obtain investment from US investors and venture capitalists (VCs) which offer better terms and valuations than Australian investors.
- Sell to some of the largest US organisations which would be difficult if the company wasn't formally headquartered in the US. Large US organisations also see working with small cutting edge startups as a competitive differentiator versus Australian companies which are traditionally risk averse and would rather buy less cutting edge technology but more tried and tested technology used by other companies first.
- Get acquired or sold to a US company. Some companies will not acquire any company that isn't headquartered in the US.

---

[13] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

[14] https://www.firstbase.io

Whilst the Australian government might see Australians forming a company overseas as evading corporate tax, these technology and cybersecurity companies are typically in build mode which means the company is losing money, not making a profit so there will be no company tax to be paid anyway. Having the individuals working for a US headquartered company being tax resident in Australia means that payroll and income taxes are remitted to the Australian government rather than the US government. Moving an Australian headquartered company or other globally headquartered companies to be Delaware, US headquartered is a common thing done today by numerous companies and is referred to globally as a "Delaware flip"[15]. I would estimate that simply changing an Australian headquartered company to be a US headquartered company can add 40%-60% to a company's valuation right away. In my view, this is something that should be encouraged and facilitated by the Australian government and that the focus on an Australian sovereign capability should be on having a high number of skilled and experienced cybersecurity professionals in Australia rather than having Australian headquartered cybersecurity companies.

Australia should look to create a cyber focused investment fund under the Future Fund that emulates Singapore's ISTARI (a subsidiary of Singapore's Temasek sovereign wealth fund) to accelerate global cybersecurity companies building a presence in Australia and to invest in Australian staffed cybersecurity companies.

Whilst I've laid out a number of strategies above to have more skilled and experienced cybersecurity professionals in Australia, another way is to emulate how ISTARI, which is a subsidiary of Singapore's Temasek sovereign wealth fund, operates. ISTARI invests[16] in global and fast growing cybersecurity companies in order to receive both returns on investment as well as encouraging or requiring the companies they invest in to have operations in Singapore. This is something that Australia's Future Fund could seek to do either directly or via a cybersecurity focused subsidiary. The United States government also has a variety of mechanisms in place that allow them to accelerate innovation in critical areas. Examples include:

- Defense Innovation Unit (DIU) - A DOD organisation made to accelerate "the adoption of commercial and dual-use technology to solve operational challenges at speed and scale"[17].
- The Defense Advanced Research Projects Agency (DARPA) - "A research and development agency of the United States Department of Defense"[18].
- Intelligence Advanced Research Projects Activity (IARPA) - As above but for the US intelligence community.
- In-Q-Tel - A government not for profit venture capital firm - Focused on investments in companies to equip the US intelligence community "with the latest in information technology"[19].

---

15 https://www.lathamdrive.com/resources/insights/doing-the-delaware-flip-why-and-how-do-non-us-companies-re-incorporate-in-the-us

16 https://istari-global.com/investor/

17 https://www.diu.mil/

18 https://www.darpa.mil/

19 https://www.iqt.org/