Recommendations for the 2023-2030 Australian Cyber Security Strategy

An Independent Contribution

[redacted]

I acknowledge the natural resources of this land which we tap as the foundation of this society; the traditional owners of the land this article was written on, their leaders past, present and future.

Question 1 - What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

Summarized list of ideas I would like to see included

1. Regulate responsibilities of cyber security and software vendors
2. Ban cryptocurrency to stop mass ransomware and extortion

Recommendation 1: Regulate responsibilities of cyber security and software vendors

The cyber security industry is part of the problem. As a multi-billion dollar industry, we profit off the vulnerability, fear and insecurity of the technology we produce, and claim to protect.

Many of the breaches that have occurred from ransomware campaigns as well as foreign government intrusion used vulnerabilities in security products (such as small medium business firewall products like fortinet, sonicwall, zoho, cisco, sophos, according to the CISA known exploited vulnerabilities catalog). As an industry, we advise organizations and consumers to purchase security products; in return, vulnerabilities in those products get them breached. That is akin to fire departments also being the arsonists.

Companies that provide cyber security products and services should be enforced to comply by a unified government standard that ensures their Software Development Life Cycle puts security at the leftmost (from the design phase) through to rigorous security testing and assessment before launching their products and services; and that their corporate IT environments and policies are upheld to a standard that prevents compromise and encourage accountability. Failure to do so should put them out of business in Australia.

Large tech companies that create products and services used on an infrastructure level across organizations (such as Microsoft, Apple and Google) are also part of the problem. The ubiquitous nature of the products created from these companies (ie. Microsoft Windows,

Microsoft Exchange, Active Directory) means that vulnerabilities in internet-exposed services play directly into the mass exploitation business model of Ransomware as a Service and other organized criminal gangs.

If organizations have to pay premiums for access to features that enable audit logging, single sign on, multi factor authentication and other security controls to those software which are insecure by design, we end up with a cyber ecosystem in which the low-budget small and medium businesses, public sector entities, not for profits, schools and healthcare organizations are the ones most vulnerable, and large private enterprises have enough money to pay for cyber insurance and PR teams that are expert at off-playing the aftermath of large data breaches. Such is the cyber ecosystem of Australia today.

Recommendation 2: Ban cryptocurrency to stop ransomware

Cryptocurrency is the gift that gives on giving cybercriminals. 100% of large ransomware payments to organized cyber crime gangs operating Ransomware-as-a-Service are done through cryptocurrencies. In the last five years, Australia organizations have increasingly become more victimized to ransomware attacks. It is more than fair to say that cryptocurrencies such as Monero and Bitcoin power most of the cybercrime underground financially.

In recent months, the US government has taken proactive steps to disrupt the cybercrime ecosystem by shutting down cryptocurrency mixer services, cryptocurrency exchanges and sanctioning related individuals. This "go after the money" approach is working, but it is not working fast enough - millions of dollars are still being pumped into criminals' wallets every month. To stop the flow of money at its source, cryptocurrency should simply be banned.

The latest "Web 3" movement has powered nothing but scams and fraud. The biggest difference between our current banking system and the use of blockchain as a financial backbone is that once money has been transferred out, it cannot be undone. All blockchain systems are immutable, and the rise of Web 3 and NFT based investment scams robbed thousands of Australians of their livelihoods.

In the looming existential threat of global warming, there is no excuse to not ban the technology that wastes terawatts of electricity to generate a virtual currency that powers the entire cybercrime industry.

Question 2 - What legislative or regulatory reforms should the Government pursue to: enhance cyber resilience across the digital economy?

(selected questions only)

a - Appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy?

Regulation and potential legislation. Stricter for larger enterprises, and more forgiving for SMEs. While compliance to security standards does not and often will not result in a high level of cyber security posture for organizations, it's a starting point to ensure all organizations have given thought to protecting their digital assets.

For example, mandating smaller organizations to produce annual assessment and improvement of their cyber security posture according to the ACSC Essential 8 would ensure a baseline level of cyber security understanding among all organizations in the economy. A hefty fine should be introduced for not doing so, for which the fine should cost more than the price of conducting such an activity), for an appropriate level of enforcement.

The starting point needs to be low, as there is a big skills gap in the industry, and many security products and services are very expensive; the goal should be for ensure every single organization has involved their business leadership and relevant IT, software development, marketing, operations and security personnel in the conversation and produce documentation that they have assessed and understood the cyber security risks that their organization faces, and have addressed whatever they are able to.

c - Should the obligations of company directors specifically address cyber security risks and consequences?

Yes. For many companies, cyber security risks and consequences are not considered consequential to the board, but have to be translated into business risk in terms of financial and reputational risks. However, it is a unique class of risk in that the consequences of stolen data and compromised systems go beyond the scope of their business. All businesses have relation to other entities, be it end consumers or other businesses. Cyber security breaches often have a cascading effect (such is the case of the Medibank breach) that lead to the potential for personal harm (e.g. via blackmailing, identity theft and fraud), and other businesses being breached as a result of their upstream provider.

f - Should Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

Yes, the government should prohibit the payment of ransoms and extortion demands by cyber criminals by both victims of cybercrime and insurers, under all circumstances.

i - What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

It would by large reduce Australian organizations as victims of ransomware and extortion. Ransomware gangs, like most cyber criminals, go for the lowest hanging fruit. If there is sufficient friction in the process of victims to pay funds for legal reasons in a certain country, attackers are more likely to avoid targets in said country.

It is not unlikely that companies will still get attacked, since there are ways to pay in cryptocurrency that are untraceable to the victim; therefore they will be encouraged to circumvent laws and keep things quiet that way. However, if cryptocurrencies are banned altogether, it will be very difficult for them to obtain such funds within Australian shores.

One notable edge case to consider are life-threatening scenarios; on one hand, emergency services and healthcare organizations that cannot access their computer systems by paying ransomware could face disastrous consequences when hacked. On the other hand, if the exception to the law of ransomware payment prohibition is healthcare and emergency services, attackers are more likely to _only_ target those organizations, which from a harm reduction perspective is extremely counter-productive; cyber security in the healthcare sector is harder than in other sectors as availability to data and systems for patient care is the primary goal, which must be placed above all else. **Hence if ransomware payments are to be strictly prohibited, it is better to do so with no exceptions** as to not single out some organizations to make them more likely to be attacked.

g - Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Yes. The Government should leave no ambiguities when stating its stance against payment of ransoms and the legal boundaries of such.