Market Incentives and Cyber Security: Fixing the Broken System Before It Breaks Us

Submission to the public consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

UNSW Institute for Cyber Security (IFCyber) and MDR Security

Is it possible to use the free market to drive the right incentives for organisations to prioritise cyber security appropriately? This was the subject of a recent discussion hosted by the UNSW Institute for Cyber Security (IFCyber) in partnership with MDR Security, bringing together leaders from government, industry and academia. Although discussions were held under Chatham House Rule, we believe many of the discussions are relevant to the development of Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. We consider that market incentives can play a major part in Shield 1 (Strong businesses and citizens) and Shield 2 (Safe technology).

In particular, this submission provides material relevant to the following questions:

8. How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?

11. Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?

16. Which regulations do you consider most important in reducing overall cyber risk in Australia?

19. How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?

Participants agreed that market incentives are important, but the approach needs to be tailored for different audiences. There are some encouraging examples of the use of market mechanisms in other industries – for example, free range egg producers charge a premium for their product, and many customers will actively choose such products because of their perceived benefits.

Government can play a variety of roles in driving the desired behaviour – by defining voluntary standards to inform consumers like the IoT labelling regulations currently under development; by using Government procurement rules to encourage specific standards and certifications, such as mandates like IRAP assessment for systems that handle Government data and DISP membership for defence supply chain companies; and ensuring transparency and accountability of organisations to their stakeholders on how well they are managing cyber security risk. One example of the proposals was to change ASX listing rules to link board bonuses to cyber security outcomes. Government could also consider how the tax system could be used to encourage certain behaviours though the use of targeted incentives, tax reliefs etc.

Education was also seen as vital. Generic campaigns can not only raise awareness amongst consumers to ask the right question, but also potentially create a societal expectation of being cyber secure – the example of free-range eggs mentioned earlier is a good example of the impact what social pressure can do. There is also be a need for more focussed guidance for different end-user communities to help them to make appropriate risk-based decisions about how they choose and engage with technology.

Insurance was suggested as another key ingredient, with the expectation that it could encourage investment in cyber security to reduce premiums. This was previously observed in the maritime industry, where requirements placed by insurers drove shipping companies to implement effective anti-piracy measures. However, it was generally felt that today the cyber insurance industry is not functioning effectively. This could be due to a lack of appropriate data to allow insurers to price risk, as well as concerns around escalating threats that are driving premiums up to unaffordable levels. The root causes of this market failure are not clear, and further research would be useful on this topic.

Ultimately, it was generally agreed that market incentives have a role but can only go so far; there will be a need for government to regulate to mandate certain behaviours, backed up by the credible threat of strong enforcement and penalties. It was noted that it was the threat of directors going to jail that made companies take workers health and safety seriously. Recently we have seen regulators pursuing organisations for significant financial penalties after major data breaches, but do we need to go further with potential criminal action in cases of gross negligence that results in a major cyber incident?

When discussing the targeting of such stronger regulation, some suggested that it should be targeted towards the upstream providers. While the Department of Home Affairs has not directly asked about this in its consultation, the consensus from our discussion was that a key goal should be that products and services are secure-by-design as a matter of course. Suppliers need to be incentivised to ensure they do not sell something that is unsafe, although, given that this duty of care also needs to extend to vetting of onward supply chains, there may need to be some flexibility in assigning responsibility.

Cyber security is not just an IT issue; it is a shared responsibility and an economic imperative – only by ensuring resilience can we confidently adopt new technology and realise its benefits. The discussion underscored that the next horizon of the cyber security strategy will need to use a mix of incentives, including regulation, market forces, and cultural change, in order to realise the Government's objective of building a secure and resilient digital economy.

We thank all the participants for their frank and valuable contributions to the debate, and hope that this summary will be helpful in the development of Horizon 2 of the Australian cyber security strategy.

[redacted]
MDR Security
[redacted]

[redacted]
UNSW
[redacted]