

8 February 2023

Australian Government

Department of Home Affairs

[auscyberstrategy@homeaffairs.gov.au](mailto:auscyberstrategy@homeaffairs.gov.au)

**RE: 2023-2030 Australian Cyber Security Strategy**

The context has already been set by news headlines in 2022, and the profession, as well as the public, are now largely aware of the heightened threats and impacts associated with weak cyber security. The conversation is quickly shifting from awareness to a stronger plan of action.

However, there is no consensus on what the actions should look like. As soon as we dip below the truisms available at the highest level like the fact we need to do better and doing better is a responsibility shared between government, businesses, and individuals, it gets much more difficult.

***1. Harmonise standards***

There is much to be said about the harmonisation of standards and it should be a key area of focus to streamline the challenge understanding what needs to be done. Even within the profession everyone has a mixed bag of favourites. Of course, what organisations need to do will depend on their unique context and risk appetite, but standards do drive improvement.

There is one international standard for cyber and information security, ISO/IEC 27001, although government and industry seem intent on reinventing standards at a national or sector level. Cyber security is a global challenge, and we should be influencing it on a regional and global level.

This can be achieved through ISO and the national standards organisations that already exist in the world to address historical challenges like safety, along with the accreditation and certification organisations made up of skilled professionals not yet fully utilised on the cyber challenge.

National, state and sector-based regulators should recognise existing standards and seek only to augment to the extent necessary. APRA CPS 234, DISP and SOCI reforms go some way in doing this, but they do not go far enough. Sector based schemes can be developed to augment ISO/IEC 27001.

Of course, a baseline standard like ISO/IEC 27001 may also need to be augmented by more technical standards in certain areas like software development, IoT and AI/ML. This is to be encouraged. Even more importantly, the government needs to harmonise fraud controls that require retention of identity documents with privacy laws that seek to minimise stores of sensitive personal information.

Naturally there is also a question of right sizing. Whilst ISO/IEC 27001 is the most practical and extensible cyber security standard in my view, it may remain a challenge for small businesses. Small businesses will instead need to rely on their supply chain and secure defaults.

## ***2. Increase supply chain security***

Supply chain security has remained a challenge with many organisations dependent on third-party technology companies cloud or otherwise. Most standards already cover the topic of supply chain security. In practice, organisations fail to identify the depth of their dependencies and protect themselves from breaches that first impact their suppliers.

A shift back towards sovereign capabilities has begun occurring over the past few years in search of greater supply chain assurance and reduced foreign interference. Standards and credentialing of suppliers through third-party audits against standards will help the right technology propagate.

There is a role for government to procure proven Australian cyber security technologies, and a role for government to subsidise the cost of third-party audits should be considered to encourage suppliers confident enough to increase transparency.

## ***3. Increase software security***

The focus of cyber security must over time shift back away from people and general awareness to secure technology. Awareness is good for problem identification and as a stop gap measure, but awareness is not a viable long-term counterbalance to vulnerable technology and weak processes.

Further investment must be made in securing the software development lifecycle, specifically the hardware, firmware, software applications and databases that occupy cyber. Knowledge of common weaknesses, tests and mitigations that address root causes must all become common.

Not only should we be sharing threat intelligence, but organisations should also be sharing information on product tests and test results and then working with suppliers (and the open-source community) to address root causes in the underlying software frameworks and libraries.

## ***4. Innovate***

Time and innovation will be required to address the cyber security challenge and that innovation must be Australian if we are to address supply chain security as well as capitalise on opportunities for economic prosperity. No doubt, government and big business need to be more willing to adopt local capabilities. Some lead in this area while other lag and 'play it safe'.

This extends to understanding the impacts and opportunities presented by developments in machine learning and artificial intelligence (AI). AI will inevitably play a large role in providing assistance in areas like virtual standards harmonisation (in lieu of immediate co-operation), threat detection and vulnerability identification. Australia can catch-up.

## ***5. Do not create another bureaucracy***

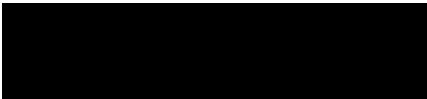
There is much that will be said about what to do -- not enough will be said about what not to do. Promoting security awareness as a panacea is blind to root causes. Professionalisation of the cyber security industry with yet another "authority" and new certification programs is a waste of time.

There are many ways to get into cyber, there is a skills shortage, there is a lack of diversity where diversity of thinking is essential. Professionalisation is a problem that is solved by the market, reputations, and optimal recruitment processes. Any new authority and certification program at this point will risk fostering group think and hindering instead of helping achieve better results.

***6. Increase trust & transparency***


Cyber security is in some ways a dark art, but it need not be. If we can reach an agreement on cyber security standards (even if we do not unanimously agree with every aspect) then independent third-party audit and assessments can create transparency and built trust – and just as importantly encourage corrective action as will prove continuously necessary as new threats emerge.

Kind regards,



**Andrew Robinson**

Co-founder & Chief Security Officer  
(ASD IRAP, ISO 27001 LA, CISSP, CISM)  
*6clicks*



Melbourne, Australia  
[6clicks.com](https://6clicks.com)