CSCAU's submission to the 2023-2030 Australian Cyber Security Strategy

April 14, 2023

This submission to the 2023-2030 Australian Cyber Security Strategy from Cyber Security Certification Australia Pty Ltd (CSCAU) is made considering our experience in improving the cyber resilience of Australian small and medium sized businesses.

CSCAU is an independently owned and operated certification authority focusing on uplifting the cyber security maturity of small and medium-sized businesses (SMBs). Our current product offering is multi-tiered cyber security standard and certification scheme which can be adopted easily and progressively by SMBs.

As an organisation founded with the sole objective of improving the cyber resilience of small and medium sized businesses and securing critical supply chains, we see this dialogue as mission critical and welcome the consultation with industry on how to most effectively develop approaches to make Australia's digital economy the global gold standard in cyber security.

A summary of our recommendations is provided below. The supporting analysis and context are provided in the remaining document.

Recommendation: Government endorsed and supported private certification schemes.

Cyber Security Strategy Discussion Questions

Q15.a What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

As mentioned in the ABS Counts of Australian Business (2022), SMBs comprise of 99.8% of all businesses in Australia. In essence, uplifting the cyber security of SMBs effectively presents Australia an opportunity to address a large cyber security gap.

From our experience and interaction with SMBs across the sector, the SMB cyber security gap stems from two obstacles.

1. Cyber security adoption for SMBs are relatively complicated due to increased cyber incident frequency and evolving threats

Small and medium-sized businesses are frequently targeted by attackers, including state attackers. The Australian Cyber Security Centre estimated that 150,000 to 200,000 small office or home office routers were vulnerable to compromise.

Recent statistics from the Australian Cyber Security Centre show:

- Average cost of cybercrime has risen by 14% from 2020-2021 to 2021-2022.
- Small businesses have an average cybercrime cost of $39,000.
- Medium-sized businesses have a higher average cybercrime cost of $88,000.

Meeting these average cybercrime costs may be difficult for small and medium-sized businesses while continuing operations.

The threat environment is also rapidly changing. For all organisations, this requires additional resources to ensure their cyber security practices are up-to-date and able to manage new risks.

For SMBs, it can be difficult to devote resources to modify or update their systems to manage these emerging cyber risks. This makes it difficult for small and medium-sized businesses to be able to develop mature cyber security practices.

2. Lack of incentives for small and medium-sized businesses to adopt cyber security

More regulation is not the answer for SMBs, and it is administratively inefficient. We all know that the vast majority of SBMs are not members of their applicable industry and trade associations, so they too are not the lever to improving SMB cyber capabilities and resilience. The real and practical incentive or driver will always be for 'commercial' reasons and the added motivation of being an important supply chain partner is also a powerful driver.

The limited resources of small and medium-sized businesses also make it difficult for voluntary adoption of cyber security practices to occur.

Further, from a consultancy perspective, it can be difficult to engage with such businesses to uplift their cyber security if there is no incentive. This lack of incentive presents an existing gap that needs to be remedied.

Typical solutions to this gap involve regulation. Mandating cyber security expectations for small and medium-sized businesses is costly and may be inefficient.

Instead, an incentive may be offered by focusing on their role in supply chains. The number of small and medium-sized businesses means that these businesses form an essential part of Australian supply chains. Their cyber security will support the securing of these supply chains.

Recognising their important role in securing supply chains can encourage small and medium-sized businesses to uplift their cyber security. By securing themselves and their supply chain, this may prevent incidents that disrupt their operations and earnings.

However, this potential incentive of protecting future earnings is only feasible if the approach to uplifting cyber security is accessible and fit-for-purpose for small and medium-sized businesses.

Recommendation: Government endorsed and supported private certification schemes

Building on discussions from the prior Cyber Security 2020 Discussion Paper, the accessibility and relevance of a cyber health mark for small and medium-sized businesses was recognised, such as by AustCyber, Google, and Office of Victorian Information Commissioner.

As recognised by the Council of Small Business Organisations Australia in an earlier discussion paper, a simple health check per se may not be sufficient in encouraging cyber security uplift in small and medium-sized businesses.

Instead, we believe that the current gaps in cyber security in SMBs may be met through industry-maintained private certification schemes. Such schemes will allow businesses to easily certify their cyber security maturity against industry expectations. Certification will require evidence of cyber security maturity from SMBs encouraging cyber security uplift.

Another key advantage gained is the speed in effecting change. By relying on certification schemes from private enterprises, the Australian Government will be able to nimbly leverage the existing efforts of agile private enterprises while remaining independent. These private enterprises will be able to leverage and adapt to newer technologies and threat environment changes.

Relying on private enterprises' certification schemes will complement existing Australian Government and Australian Signals Directorate's investment into the cyber security of small and medium-sized businesses, such as through REDSPICE.

Existing certification/standards schemes with a similar infrastructure (private or separate state enterprise endorsed by Government) implemented in other industries such as the Australasian Recycling Label.

However, the success of these certification schemes will be reliant on the input, support and endorsement of the Australian Government.

The Australian government endorsement of private industry-led certification schemes will further support and give credibility to these schemes.

The opportunity for hundreds of thousands of Australian SMBs to have access to a plain English web platform to obtain a highly affordable and user-friendly cyber certification, whilst being encouraged and supported by their major customer/buyer through the process would be major step forward to raising Australia's cyber security posture and indeed, for our national economy.

It would give Australian SMBs a ticket to play the big game and be seen by their bigger customer as a 'safe' member of any supply chain that is commercially important to their business.

This will further bring about cyber security uplift for small and medium-sized businesses – at scale and at pace with the unique frequency of change in the cyber security sector.

Contributors

- Prof Ryan Ko
- Prof John Swinson
- Adj Prof Nick Tate
- Adj A/Prof David Ross
- Mr Paul Russell
- Ms Elinor Tsen
- Mr Peter Maynard
- Mr Graham Maynard OAM
- Mr Lani Refiti

Contact details

Email: admin@cscau.com.au