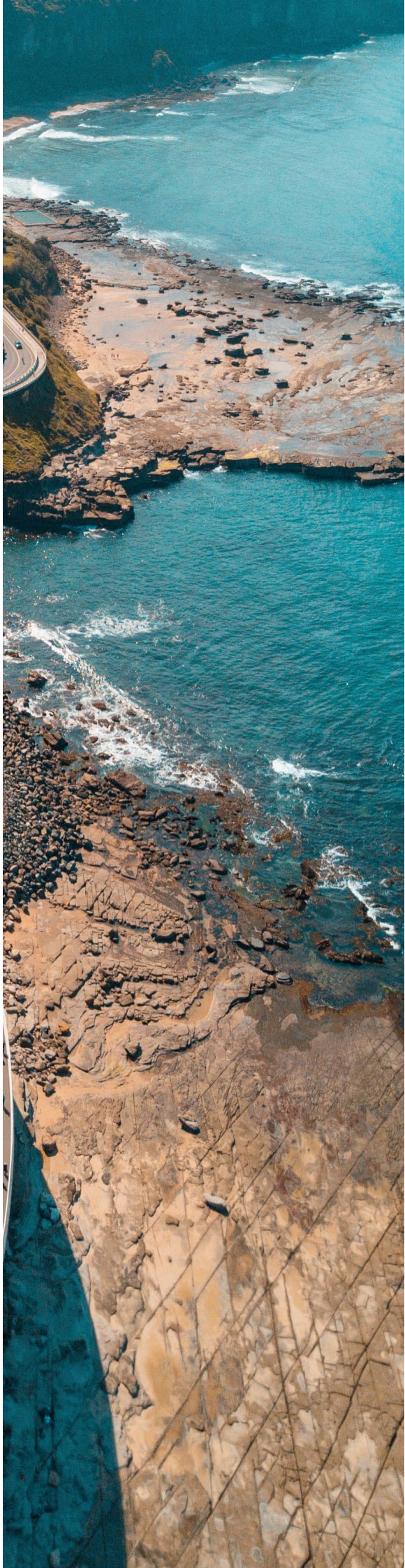
Submission

By Khoa Duong (Industry Protective Security Leader)

Strengthening Australia's cyber security regulations and incentives

August 2021

Table of Contents



Executive Summary

Submission Goal

The goal of this submission is to present my views, based on my industry experience and knowledge, regarding the issues with and possible solutions for the topics presented within the 'Strengthening Australia's cyber security regulations and incentives' paper.

Areas of Focus

My responses are covered by the areas of focus below

Expectations and Guidelines

Addressing Smart Devices

Cyber Strategy Gaps

Recommended Actions

I recommend the following actions be considered in each area of focus

Mandate a cyber security framework with a clear minimum baseline	Set and define minimum security controls for smart devices	Embed cyber security content in the curriculum at all layers of education
Provide further support to SMBs as part of the suggested health check system	Implement smart device labelling to improve consumer understanding of the risks devices pose	Introduce guidelines for risk management or abandon risk-based approach to compliance
Raise the posture of Government departments above baseline controls that are implemented	Deploy a secure enclave for smart devices to ensure the security of existing insecure devices	Increase ACSC response times and improve federal coordination for large cyber security incidents

Introduction

It is my firm belief that improving Australia's cyber security posture and capabilities is a responsibility and opportunity shared at all levels nationally between governments, businesses, and the community.

I am pleased to offer my feedback on the discussion paper, 'Strengthening Australia's cyber security regulations and incentives'. As an experienced professional in the cyber security industry and having worked across multiple sectors and businesses of all sizes, I welcome the opportunity to share my unique point of view on these issues. In this response, I highlight the issues and possible solutions for many of the topics presented in this paper relating to Australia's cyber security regulatory frameworks, the risks and challenges of smart devices and some additional gaps in Australia's cyber security strategy.

It is my firm belief that improving Australia's cyber security posture and capabilities is a responsibility and opportunity shared at all levels nationally between governments, businesses, and the community.

I see an abundance to learn on how to further develop Australia's cyber security resilience from previous Government initiatives and industry responses to cyber incidents. The Government must look toward preventing imminent threats by strengthening regulations from lessons previously learnt to protect Australia considering the rapidly growing digital economy fuelled by the implications of the COVID-19 pandemic.

My response to this paper addresses the following key points:

- Setting clear cyber security expectations through a government-endorsed framework that can be applied to Australian businesses.
- Implementing a mandatory minimum baseline of cyber security controls with clear implementation guidance that is less open to interpretation.
- Considering the impacts of regulation towards small to medium businesses which are vital to improving Australia's cyber security posture and may require additional support.
- Implementing minimum standards for smart device controls and appropriate labelling, as well as the issues in policing this.
- Addressing Australia's cyber security management capabilities, such as lack of training and awareness, risk-based approaches, minimising red tape, and national incident response approaches.

Clear Expectations and Guidelines

Issues with the existing framework

At present, Australian businesses hoping to identify and comply Australian cyber security 'best practice' are met with a complicated ecosystem consisting multiple different frameworks and regulations and no defined guidance from the government on which to follow. In addition to this, Australian companies are required to understand and monitor multiple pieces of legislation to ensure they are meeting their requirements.

The current state of Australian cyber security guidance, such as the Australian Cyber Security Centre's (ACSC) Essential Eight, focus on 'best practice'. This focus creates a significantly high barrier for entry for larger Australian businesses and makes meeting these goals essentially unattainable for Australian small to medium businesses (SMBs). In addition to this, the current guidance leaves the implementation of these controls open to interpretation, which has led to inconsistent cyber security maturity across Australian businesses. If you also looking at the Australian National Audit Office's audit reports on cyber resilience, it also highlights the challenges that Government have with this, let alone the private sector.

I have also perceived that, fuelled by a lack of mandatory regulations in the cyber security space, cyber security teams within Australian businesses are struggling to garner adequate funding and resources to appropriately implement adequate cyber security controls.

Clarifying expectations to drive adoption

The Government has shown that it perceives cyber security risks to Australian businesses as a critical factor to be addressed, however, have not taken appropriate steps to address these risks in a timely manner. In order to improve the cyber security practices of Australian businesses within an appropriate timeline, the Government must take a more forceful approach to mandating adoption.

To this end, I recommend the implementation of a government-endorsed framework that can be followed by all Australian businesses to appropriately understand and meet their regulatory cyber security requirements. This framework must contain a mandatory set of clearly defined, practical and relatively stable minimum baseline cyber security controls and clear guidance regarding the appropriate implementation of these controls. I feel that by improving the clarity of expectations for

Australian businesses and mandating a minimum level of compliance, Australia will be able to raise our cyber security posture to an overall adequate level within a timeframe that appropriately reflects the associated risks. We also need to ensure there is practical guidance on the implementation. If we look to some of Government's frameworks, such as the Protective Security Policy Framework (PSPF), my experience tells me we do not do enough to help organisations approach the implementation correctly.

As with any mandatory requirements, it will be important to provide adequate time and resources to businesses to implement these guidelines before consequences are faced. Having said that, this timeline could be shortened considerably for businesses working for Government, who already have some mandatory requirements.

Challenges faced by SMBs

As work continues to increase the overall cyber security posture of all Australian businesses, there is a significant gap created by Australian SMBs. Considering that even large corporate enterprises and Government agencies struggle to appropriately implement the existing guidance (such as the Top Four and Essential Eight), this has become an impossible end goal for a majority of SMBs. This lack of adequate cyber security in SMBs also adds to the existing issues with supply chain security for all Australian businesses. It is my opinion that Australia's cyber security posture cannot improve to an appropriate level without addressing the issues faced by Australian SMBs. While I agree that the proposed 'health check' system would be beneficial to large Australian businesses when selecting vendors in their supply chain, I do not believe it adequately addresses the struggles faced by Australian SMBs attempting to uplift their cyber security and risk management practices. To achieve this, I would strongly recommend that further support is offered to SMBs as a part of this health check, such as strategies to further improve their posture and information on the key gaps in their existing controls. We should also offer free health checks to get them on the journey.

Government leading by example

While the Government has previously released limited guidance on cyber security best practices for Australian businesses, the Government's own implementations of these best practices is significantly varied and mostly immature, as flagged in annual ANAO audits. In order to appropriately demonstrate the importance of implementing strong cyber security controls to Australian businesses, I believe the government should have a strong, coordinated approach to their own cyber security implementation. Prior to mandating compliance with a framework for Australian businesses, it is vital that the Government raise the posture of their departments above the minimum baseline controls that are to be implemented. This will be vital in providing guidance to Australian businesses and showing that Australia is dedicated to becoming a world leader in cyber security.

Concerns of regulatory overhead

With the introduction of any mandatory expectations in regulations come additional requirements for regulatory oversight and auditing. While I see the absolute need for mandating minimum expectations in the cyber security space, the Government must be cautious in its approach to avoid overwhelming its systems. Parallels can be drawn here with the introduction and rollout of the PSPF to non-corporate Commonwealth entities, which has seen significant issues with multiple agencies still not implementing the framework correctly. To avoid the issues faced by implementation, the Government must provide adequate understanding and support for businesses in the implementation of the minimum baseline expectations, whilst also further providing support through a consulting and assurance regime.

Addressing Smart Devices

Implementing smart device controls

Australia has already implemented mandatory control frameworks in several industries. Businesses in construction and manufacturing are actively complying with mandatory requirements for the safety of Australian consumers. Consumers are also accustomed to such requirements including passports and visa for international travel. Each of these examples were implemented to ensure the security and safety of Australians, however also highlight the challenges with maintaining consumer and public trust, such as the recent quality issues in the construction industry.

I believe that similar requirements are necessary for smart devices, to ensure that Australian consumers are both aware of and protected from the security risks presented by the smart devices they rely upon. These requirements should include minimum thresholds for security controls within smart devices and adequate labelling to show customers that a device meets the requirements. To ensure the greatest impact to the landscape, these requirements should, in the first instance, be targeted at companies selling the largest volumes of smart devices in Australia.

Smart device requirement considerations

By design, smart devices are created to achieve their required use-case for the cheapest price to consumers possible. Due to this, creating mandatory requirements for smart devices in Australia must be approached carefully so as not to disrupt the market and impact availability for consumers or result in non-compliance by major manufacturers. At the end of the day, consumers will normally always purchase the product that is perceived to be the most value for money.

Policing these requirements will also be a significant issue for the Government to solve. Even with clearly defined standards in the construction industry, issues with buildings continue to occur; this same issue would significantly impact consumer confidence in any potential labelling scheme or requirements.

In addition to these considerations, any smart device requirements or labelling implemented must be able to be action quickly enough to keep up with the rapid pace of smart device development. The Government's approach to the Evaluated Products List (EPL) as an

example, highlights an attempt to try and solve a similar problem, however, the time taken between the release of a product and its evaluation and addition to the EPL is a severely limiting factor. As smart devices are released much more regularly, the matching evaluations for smart devices need to be much faster. History shows that the Government will likely struggle with this load and pace, so any solution will need to be designed with these considerations in mind. However, the options to label could be a move to simplify the decision-making process for consumers. However, it cannot be just a simple 5 star rating scheme, as what would the criteria be, and what is the applicability period for this. Cyber threats are constantly changing and new vulnerabilities emerge all the time. Perhaps being more clear on what consumers can actually do to better protect their devices and know when support will end is the first logical step.

Whichever requirements are introduced to the smart device markets, there will likely be a cost involved in their implementation. Given the importance of pricing in the smart device market, the Government will need to find ways to incentivise manufacturers to meet these requirements. Requirements for Government-owned devices will present a market opportunity for companies, while initial subsidies or rebates may convince initial uptake. At a point, however, consumer trends regarding purchasing will be the key factor in compliance and competition.

Providing a secure enclave

Given the significant difficulties faced by the introduction of mandatory requirements in smart devices, this is unlikely to be implemented quickly. While these requirements are being considered, however, a significant number of smart devices remain active in Australian networks and present a clear and present danger which should not be ignored.

In order to address this risk, the Government could consider the implementation of a ‘secure enclave’ for smart devices in high risk areas to connect to and reduce their residual risk to other connected devices on Australian home and business networks. This enclave could be offered to Australian businesses for a small subscription, enabling them to ensure their networks are not at risk from insecure smart devices while maintaining the requirements for BYOD networking.

Gaps in Australia's Cyber Strategy

Building a culture of awareness

Cyber security awareness is rapidly becoming a topic of key priority for all Australian businesses. Delivering appropriate cyber security awareness training to staff members is extremely difficult and creates significant overhead for cyber security teams. In addition to this, workplace trainings are commonly the first examples of cyber security awareness employees are exposed to.

The lack of cyber security awareness content in curriculums throughout primary, secondary and tertiary education continues to perpetuate and exacerbate this issue. Cyber security awareness content must be presented in all layers of education, in order to adequately prepare Australians to consider the cyber security risks in their daily lives, in their workplaces and in the products they purchase.

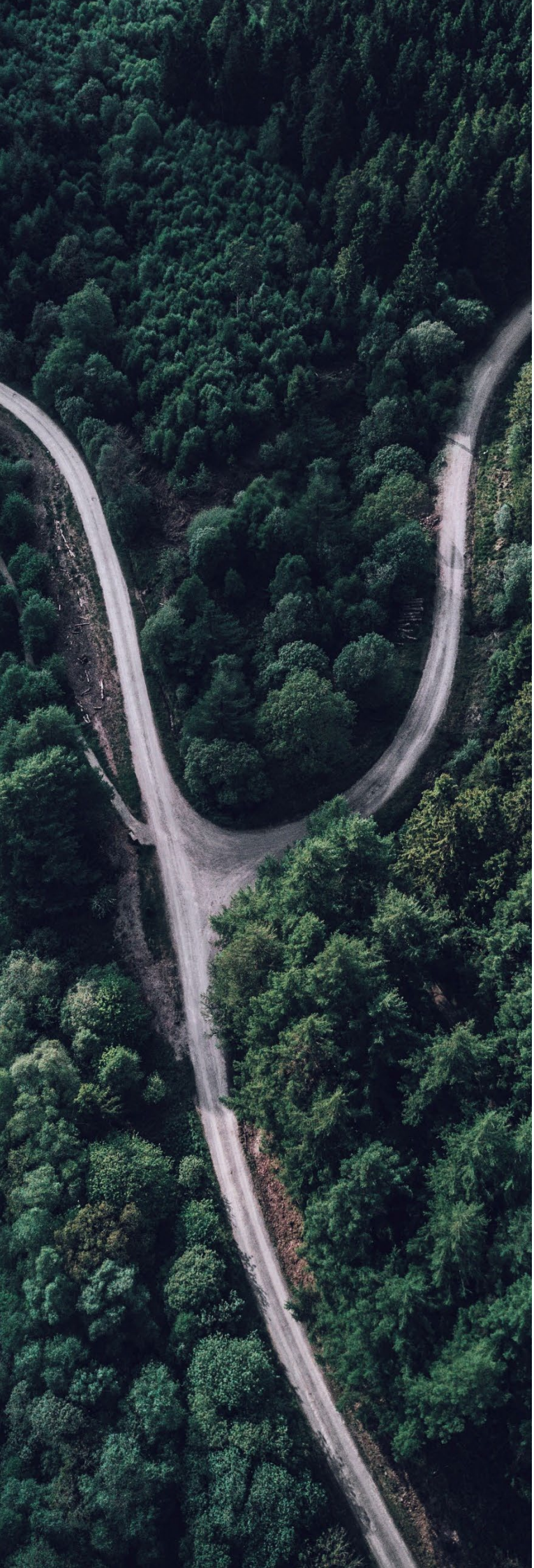
Flaws in risk-based approaches

Without a pre-determined framework for managing risks related to cyber security, Australian businesses have varied approaches to risk management. Many of these strategies are immature or inadequate and do not appropriately identify, reduce or mitigate risks. Despite this, Australia's cyber security framework continues to push a risk-based approach to legislative compliance. This duality needs to be addressed for Australia's cyber security strategy to be truly effective; either through the introduction of risk management guidelines or moving away from the risk-based approach to compliance.

Response times and red tape

It is my opinion that the current response times from Government regarding cyber security issues and incidents is too slow; hampered by excessive red tape. An example of this is the previous phishing exercise undertaken by the Government which demonstrated insufficient communications and support for businesses after the exercise.

In order to offer adequate support to Australian businesses in relation to cyber security issues and incidents, the Government must make efforts to increase its response times and reduce this red tape.

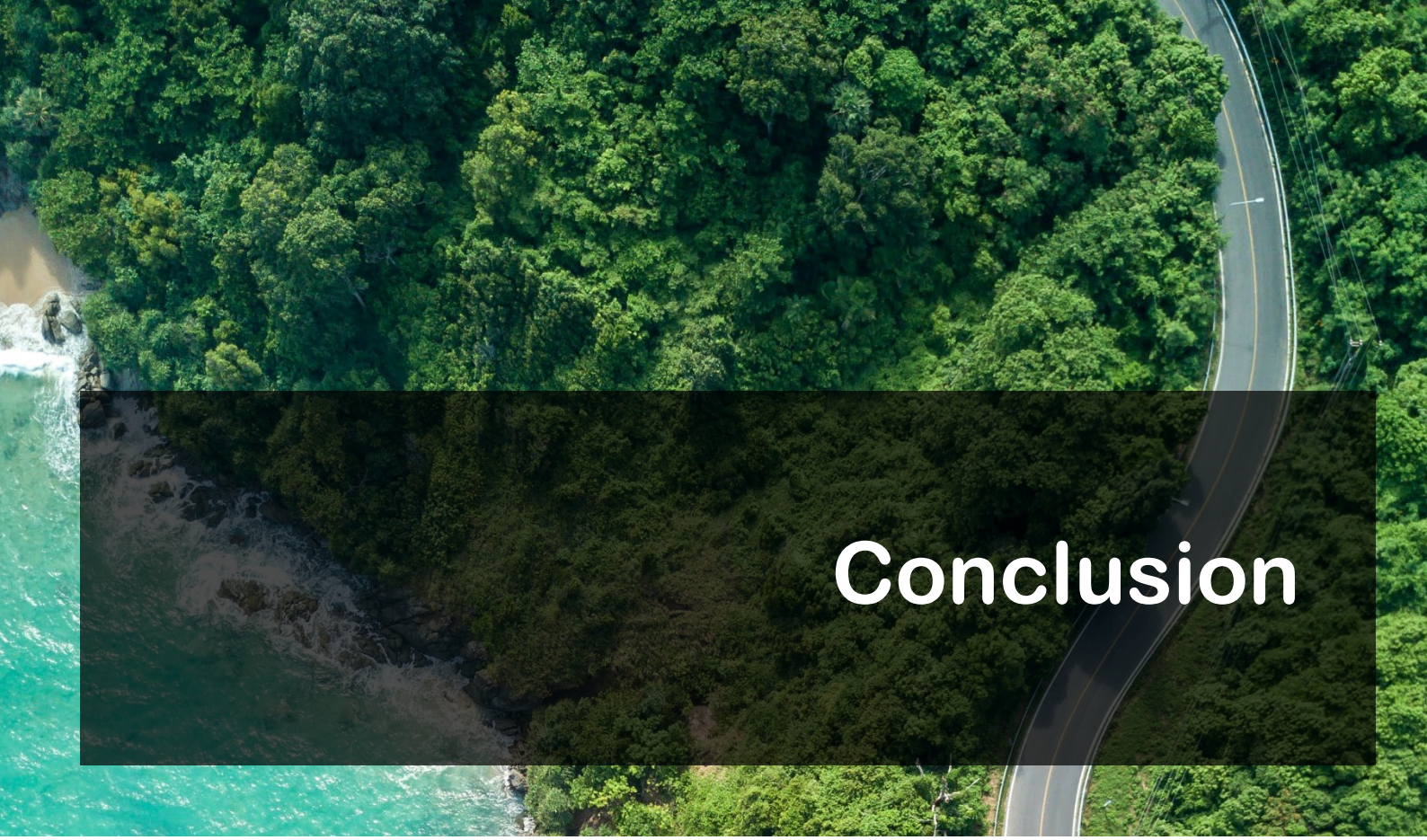


Adjusting the ACSC response model

At present, the ACSC's response model to cyber security incidents reflects that of other emergency services with state-based responsibilities and minimal federal oversight.

Due to the nature of cyber security incidents and the geographical separation of logical networks, I would suggest that this approach is inappropriate. Based on the identified supply chain risks posed by Australian SMBs and the increasing commonality of cyber incidents even in large corporate enterprises, any cyber incident could pose a significant risk to multiple other Australian businesses and sectors. As such, by limiting the response to incidents only to the varied capabilities and capacity of state-controlled resources, I believe that this approach increases the risk to Australian businesses. This can also get in the way of ensuring an appropriate response to a complex or large-scale cyber incident or threat.

In order to adequately protect Australian businesses from the threats posed by cyber security incidents, Australia's cyber security legislative framework must support a coordinated approach between states with federal oversight from the ACSC. This approach will allow for Australian businesses to more rapidly respond to emerging incidents and coordinate their responses more effectively. The legislative framework will also need to support this cross-jurisdictional approach.



Conclusion

I reiterate my praise of the Government's commitment to collaborating with industry on Australia's cyber security strategy and its goals.

While the actions taken as a part of Australia's Cyber Security Strategy have been largely on the correct path, I feel that the lack of clear and mandatory requirements has significantly impacted the adoption of the guidance provided. I feel that Australia's cyber security position has reached a state at which, without these mandatory requirements, Australian businesses will not be able to appropriately resource their teams to keep up with the growing threat of cyberattacks.

In addition to this, the complexity of the existing framework as well as the lack of specific guidance on the implementation of cyber security best practice has limited the ability for Australian businesses to improve their cyber security posture; especially so for Australian SMBs.

I applaud the Government for attempting to address the significant risks posed by smart devices, despite how difficult this issue is to fix and recommend that careful consideration be given to manufacturer adoption of these controls and the impacts to consumers. Due to the significance of these discussions, I recommend the Government may want to consider implementing a secure enclave for smart devices operating in high risk environments, which could allow for insecure devices to be used securely, while further controls can be adequately implemented.

In summary, I believe the most important actions to be taken by the Government are:

- Clarify the security approach and framework requirements, and implement mandatory baseline expectations for cyber security controls.
- Implement mandatory minimum controls for smart devices, in collaboration with manufacturers.
- Consider a secure enclave for smart devices to tackle the risk of insecure devices already in use.
- Add cyber security awareness content to education curriculum at all levels.
- Improve the response time, approach and framework for Government and ACSC in relation to cyber security issues and incidents.

In the COVID response space we see the debate around the use of vaccine passports. Perhaps a similar concept could be applied in this space, in which key service providers need to have 'passport' or 'visa', and regularly stamped as they progress into new areas or make available new products and services.