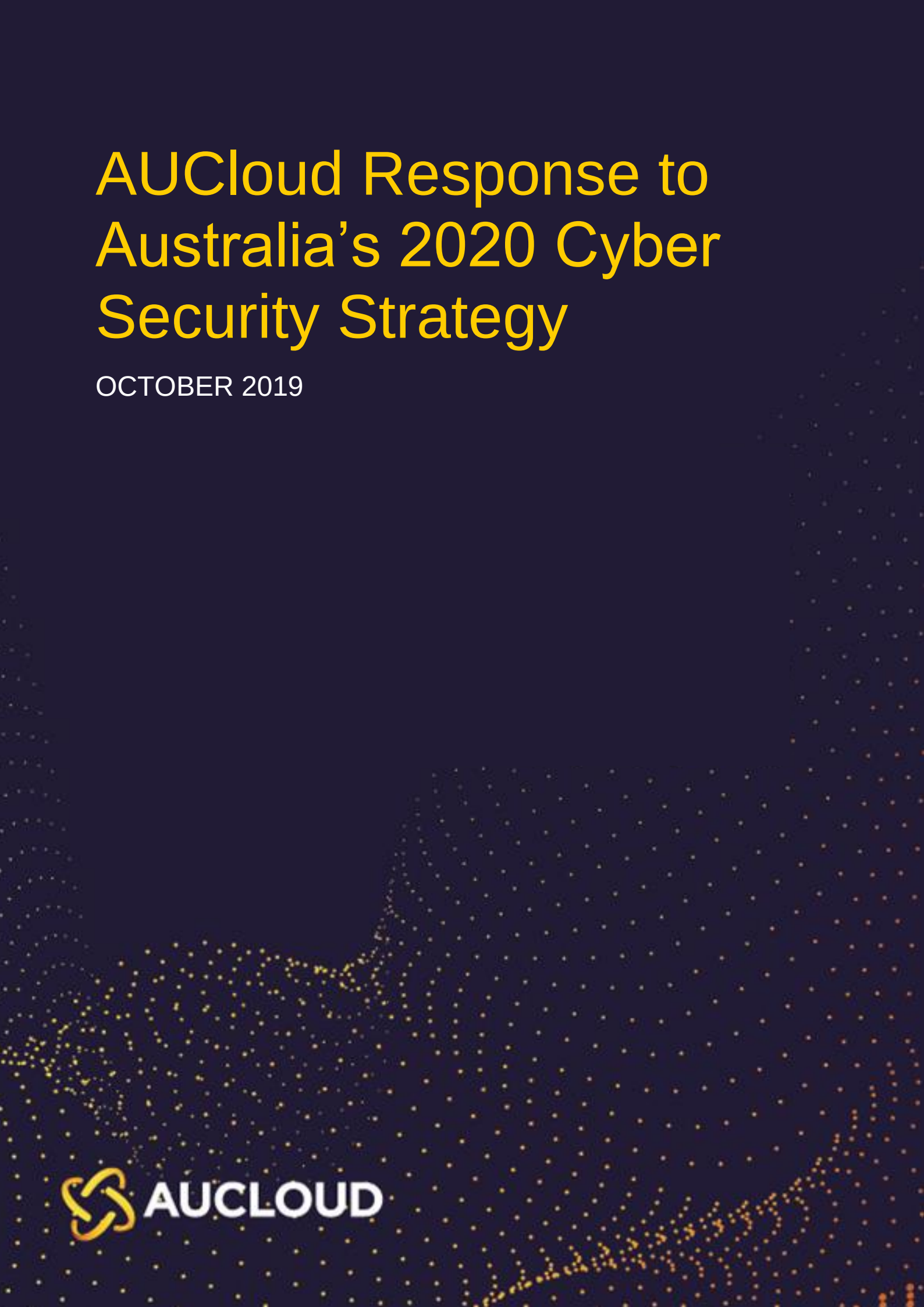
AUCloud Response to Australia's 2020 Cyber Security Strategy

OCTOBER 2019



Disclaimer

The information in this Proposal is the confidential information of Sovereign Cloud Australia Pty Ltd ("AUCloud"). Such information must confidential at all times and used solely to consider the Proposal put forth by AUCloud. You agree to take such measures to prevent the disclosure of the information as you would to prevent the disclosure of your own proprietary information, but in all cases, shall use at least reasonable care.

The information in this Proposal is correct at the time of print, and is subject to change without prior notice. The prices set out herein are indicative prices only and provided for informational purposes only. These prices are neither final nor binding upon AUCloud or any third party AUCloud reseller, and are subject to revision from time to time. For the avoidance of doubt, the price for the supply of AUCloud's products and services the subject of this proposal will be independently agreed between you and your preferred AUCloud reseller.

This is not a legally binding document and is submitted for information purposes only. Due to the forward-looking nature of this document, AUCloud's response may include information about solutions or products that may be in the planning stage of development or that may represent custom features or product enhancements. Feature and functionality cited in this document that is not publicly available or generally available today is discussed within the context of the strategic evolution of the proposed products. AUCloud is under no obligation to provide such future functionality.

TABLE OF CONTENTS

Introduction

Thank you for the opportunity to respond to **Australia's 2020 Cyber Security Strategy**.

AUCloud is a sovereign cloud Infrastructure-as-a-Service (IaaS) provider, exclusively focused on meeting the needs of the Australian Government and Critical National Infrastructure (CNI) communities. This includes Federal, State and Local Governments and CNI organisations such as telecommunications, electricity, energy, financial services and similar utility providers.

Security is core to how we operate at AUCloud.

Independently IRAP assessed to the PROTECTED level controls of the Australian Signals Directorate (ASD) Information Security Manual (ISM), AUCloud provides two independent environments: an Official Data Community Environment (ODCE) and a PROTECTED Data Community Environment (PDCE) that meet or exceed these controls.

AUCloud solutions enable customers to benefit from sovereign data protection with the scale, automation, elasticity and lower costs typically associated with global cloud offerings.

As a sovereign IaaS provider, AUCloud is owned, managed and operated in Australia. All services and data managed by AUCloud remain in Australia ALWAYS (including metadata, monitoring data and derived analytics data). All AUCloud services are monitored and operated in Australia by Australian citizens who have been security cleared to Australian Government standards.

AUCloud operates from two Data Centres: Sovereignty Zone 1 in Canberra and Sovereignty Zone 2 in Sydney, both designed to meet ASIO T4 standards for Zone 4 security.

A call for views

AUCloud Response

AUCloud submits the following response to the Australian Government's 2020 Cyber Security Strategy – A call for views paper, noting that organisations have the option of replying to all or some of the questions posed.

1. **What is your view of the cyber threat environment? What threats should Government be focusing on?**

As tools for threat actors become cheaper and more readily available, the cyber threat environment will continue to evolve at a rapid pace, often faster than Government and suppliers will be able to respond. The capabilities of nation state actors are well known although their attack surface is, for the most part, restricted to Government outcomes and suppliers. However, the primary target of threat actors will continue to be the theft of personal and financial information of individuals and companies. Affordable and low-tech attacks such as ransomware, phishing and malware will continue to rise and a greater emphasis from Government on supporting small to medium businesses and corporate Australia from cyber criminals is required. In that sense, for many Australian businesses, a mind shift to data centric protection and understanding the value of their data would greatly assist risk based decision making.

Part of that conversation will focus on the threat and ways it can be mitigated but more education is also required to assist these businesses to understand cyber security risks in the first instance. Programs such as Stay Smart Online, Scamwatch and establishment of the eSafety Commissioner have been successful in their own ways but much more can be done by Government to assist businesses in understanding the risk levels before identifying specific threats.

The Joint Cyber Security Centre's (JCSC) have been a welcome addition to filling the communication gap between Government and business. The collaboration within these communities is an ideal starting point to further the breadth of Government assistance and involvement against cybercrime. The challenge for the ACSC will be how to expand and scale these services to assist corporate Australia more broadly.

We would also expect to see more focused attempts from sophisticated threat actors to exploit the trusted relationships between businesses and their suppliers/service providers for cybercrime purposes. Any compromise of the supply chain, especially hardware and software supply chains, will make the detection and attribution more difficult.

2. **Do you agree with our understanding of who is responsible for managing cyber risks in the economy?**

Individuals and companies generally accept that doing business on the Internet comes with an inherent level of risk and that individuals and companies have a responsibility to protect themselves. The motivators for protecting themselves may vary greatly though, whether that be social conscience, industry best practice, economic motivation or legal accountability.

However, it would seem pertinent to highlight that Government's role is much more than protecting a network. Its mission should be to protect Australian's security and privacy, and the data it holds about its citizens.

At a national economic level, the Federal Government has responsibility to lead, audit and regulate best practice through related bodies such as APRA, ASIC, ASX, ACCC and others. The role of the Office of the Australian Information Commissioner (OAIC) should also be considered when considering cyber risks to the economy. The current framework that OAIC operates under is well established but as the cyber threat landscape evolves it is important that bodies such as the OAIC, and the eSafety Commissioner, are subject to regular review to maintain the necessary remit for the protection of privacy and data access rights.

3. **Do you think the way these responsibilities are currently allocated is right? What changes should we consider?**

There is no clear picture available that concisely delineates how these responsibilities are owned and/or shared. Even across Federal and State Government, agencies have varying levels of cyber maturity, understanding of their responsibilities and awareness of the risks they face. Similar to the way that cloud service providers use shared responsibility models, Government could look to create a shared best practice community through the ACSC or DTA that can offer advice on risks they face and best practice approaches for mitigating these issues. ACSC has recently authored several articles about issues facing particular sectors and these communications should continue to be enhanced.

If the Government were to consider transferring a greater portion of cyber security risk to industry and business we would expect considerable consultation and involvement from industry in shaping how this could be appropriately managed.

4. **What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?**

Government has a lead role to play. The question is however, how quickly Government can respond to address serious threats. While the ACSC has been established and can assist with nation scale threats, the industry is seeking more proactive involvement and leadership when it comes to real time incident response activities across a much broader range of issues than just nation scale threats.

Being able to provide rapid response and assistance should be a key deliverable of the Cyber Security Strategy. Similarly, any rapid response capability should be tested across a variety of sectors, possibly using the critical national infrastructure communities as a starting point. Such an approach would require enhanced levels of investment to address a much wider threat vector.

A greater focus on building systems that are on well protected sovereign platforms, where all data, meta-data, monitoring data and derived data, are guaranteed to remain in Australia under Australian law and away from external jurisdictions would further simplify complex matters when dealing with cyber security incidents. It is no secret that many Australian companies are completely unaware of the contractual details they enter into with global providers and the Government has long talked about promoting and enhancing the Australian IT sector. A renewed Cyber Security Strategy presents a prime opportunity to further highlight the need for sovereign capabilities.

In addition, establishment of an incident response marketplace, operated by either the ACSC or DTA and entered into based on zero-dollar contracts, would also alleviate a common problem of who to seek assistance from when dealing with a cyber security incident. Organisations that AUCloud deals with often highlight this as an issue that have faced, especially the inability to distinguish once incident response capability from another, with business decisions primarily based upon financial decision making.

5. **How can Government maintain trust from the Australian community when using its cyber security capabilities?**

First and foremost, the Government needs to adopt and maintain a citizen first approach. The privacy, security and impact upon the Australian public should be central to any use of cyber security capabilities. At present the cyber security industry has seen a shift away from these principles with the Government endorsing alternative approaches to the detriment of cyber security principles.

Secondly, in the case of Government or even if applied more broadly, the Government should establish and maintain credible standards with appropriate validation (the Certified Cloud Service List as an example) or a trusted community (such as IRAP or CREST) so that users (be it consumers, developers or SaaS providers) can make decisions based upon confidence that baseline security controls across people, process and technology are delivered to a specific risk level criterion.

6. **What customer protections should apply to the security of cyber goods and services?**

No general comments other than that standard consumer protections should apply equally in the case of cyber security goods and services.

7. **What role can Government and industry play in supporting the cyber security of consumers?**

A different approach is needed with the OAIC given more responsibility to introduce privacy legislation in line with GDPR. Such an approach would change the responsibility of privacy and consent in Australia from assuming consent for all rights, to micro consent arrangements based upon no default rights.

Likewise, and it may sound cliché, but industry continues to let itself down by deploying insecure or badly designed solutions for consumers. For too long security has been an afterthought in the design process but with the advent of IoT and the ever-increasing connectivity presence within our daily lives, the need for security by design and zero trust models has never been greater.

8. **How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?**

Several years ago, the UK Government introduced the Cyber Essentials scheme to guard against the most common cyber threats and demonstrate an organisation's commitment to cyber security. A similar scheme in Australia, at a non-restrictive price point, would allow a large variety of organisations to not only uplift their cyber security knowledge but also promote their commitment to cyber security principles.

Many of the building blocks for such a scheme already exist in Australia while certifications bodies could easily align with IRAP, CREST or ISO 27001 certification organisations.

The requirement for industry standards and accountability has also been a successful approach, with CPG 234 for all APRA regulated entities a good example. Links to other national bodies such as the Australian Institute of Company Directors (AICD) may also offer an opportunity to more widely introduce practical security outcomes.

9. **Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?**

Government should have responsibility to communicate high level standards such as they do regarding the PSPF, ISM, Strategies to Mitigate Cyber Security Incidents and the Essential Eight, as well as additional guides on how this can be achieved in practice. Where appropriate (based on data aggregation, high risk, high impact etc.) Government should maintain an appropriate role for audit and validation, including defining policy that minimum standards have been achieved.

The private sector can assist in these processes given the resource constraints of many Government agencies, including the ACSC. It could, for example, partake in detailed audit and validation roles with the potential to amplify the private sectors willingness to invest in these functions; similar to how CA and CPA accountants power their industries. For lower risk, lower impact areas the Government can maintain the standards and advisory role it currently performs and signal to the wider private market that the ACSC as a shopfront is open for business to support Government, private sector and consumers.

10. **Is the regulatory environment for cyber security appropriate? Why or why not?**

For the most part the regulatory environment for cyber security is well understood, especially in the banking and financial sector and regulatory schemes such as PCI DSS. Having said that, the Federal Government's current approach to providing legislative frameworks and policy, through to policy implementation and validation of best practices is highly confused with little communication or direction provided. This is evidenced through public facing programs such as IRAP and the CCSL which have been stagnate for long periods of time; as well as the vastly varying degrees of success of Federal Government agencies implementing the Essential Eight. Consequently, there is a greatly reduced level of trust and opportunity in the industry that the Government can provide credible solutions for other governments, businesses or consumers.

11. **What specific market incentives or regulatory changes should Government consider?**

A mind shift to privacy and consent legislation, like GDPR, is key. This is what really matters to the Australian public; how Government can protect us and our data, and what is in the Government's own Cyber Security Strategy that articulates this and protects individuals (as well as the industry). The OAIC should be armed with significant power and associated fines/sanctions so that focus can be applied across Government and industry so that action can be taken in the immediate term.

12. What needs to be done so that cyber security is 'built in' to digital goods and services?

An age-old question really that can only be answered by those providing digital goods and services. It's a genuine commitment to valuing security and building it into goods and services at the beginning. At some point, most likely after a significant incident, consumers will realise the value of those that do build in security as part of the goods and services they provide.

13. How could we approach instilling better trust in ICT supply chains?

The threat to supply chains and the risk of theft of intellectual property (IP) and commercially sensitive information is likely to grow in the foreseeable future. There has been significant research in this field to indicate that IP theft is higher when businesses operate abroad – whether that be due to design or manufacturing. Some countries even have domestic policies that allow their Government to access data as it transits or resides in their country. As a result, businesses should always remain vigilant and aware of how these policies may impact their business.

Within Australia, we can better instill trust by developing our own supply chains and investing in sovereign capabilities. As a business, zero trust models should be adopted so that each entity within the supply chain network is required to rely on its own investments and trained staff to mitigate risks to IP and access to data.

14. How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

Many would argue this already exists. If the focus of the question is on developing cyber security professionals for the future it most definitely starts with education. Across Australia, curriculums have started to include cyber security courses at the high school and college levels, significant work has been done at the TAFE level and need for greater emphasis on STEM disciplines is well documented. If Government or private entities wish to accelerate development in these areas, additional investment should be considered.

15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

At present, neither the economic nor legal consequences are perceived as being sufficiently significant to warrant individuals or organisations to treat the loss or integrity of data seriously and with any urgency. As a result, the market for insurance will remain limited. However, once the consequences of cyber failure increase the demand for insuring against such damages will grow. The OAIC and the Notifiable Data Breach scheme are likely to be the best avenue for capturing and measuring how effective or otherwise the cyber insurance market is.

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

At a national level, improved technologies such as DNS security (analytics, threat detection and proactive blocking) can be introduced to significantly reduce malicious activity through co-operation with service providers.

A nation scale Malware Information Sharing Platform (MISP) would also be a significant step to reducing malicious activity while also achieving the objective of rapid response from Government and industry.

Approximately 6 years ago the UK Government introduced the Cyber Security Information Sharing Partnership (CiSP) as a joint Government and industry initiative to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, to increase situational awareness and reduce the impact on UK business. Such a system should be a high priority as the sharing, storing and correlating of Indicators of Compromise (IoC) data to detect and prevent attacks, fraud or threats against ICT infrastructures, organisations or people, is mission critical for many organisations.

The UK experience of using CiSP has been incredibly positive and given Australia's geographic diversity and multiple layers of Government, such a solution would seem tailor made for the Australian operating environment.

17. **What changes can Government make to create a hostile environment for malicious cyber actors?**

It is important that the Government maintain a capability to respond in hostile environments to disrupt and take down malicious cyber actors based upon the threat. Equally important is that this capability is supported by legislation and is sufficiently transparent about how the capability and operations are maintained.

18. **How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?**

Governments and private entities should continue to work together in established channels to collaborate, share threat intelligence and, where necessary, remediate risks before they become cyber incidents. UK Government initiatives that we believe would add value to the Australian cyber security industry include:

- UK Cyber Essentials (including Cyber Essentials Plus)
- Cyber Security Information Sharing Partnership (CiSP)

19. **What private networks should be considered critical systems that need stronger cyber defences?**

Australia's Critical Infrastructure Centre operates across 8 critical sectors which have shown a need to be resilient against cyber-attacks. In addition, we would highlight the need for any cloud infrastructure supporting those sectors or Government also requiring a high level of cyber threat monitoring to be effective; in essence any, network that has a materially large-scale impact on Australian consumers.

20. **What funding models should Government explore for any additional protections provided to the community?**

The Government could establish legislation and significant penalties for the failure to protect consumer data. This will drive uptake for stronger cyber defences as well as the growth of cyber security companies. From there the Government could establish specific cyber taxes or minimum investment requirements that will improve the overall quality of private networks/IaaS.

Additionally, the Government could implement swinging tax penalties for overseas providers that operate such infrastructure and shield their profitability by establishing their intellectual property in low tax zones.

21. **What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?**

The primary constraint to information sharing continues to be the time taken for Government to make decisions and share information. It is imperative that the Government adopts agile and fit for purpose decision making processes about sharing information on cyber threats and vulnerabilities. As stated previously, a national platform for sharing threat intelligence should be a priority.

22. **To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?**

Perhaps in some cases but would not say there is a direct correlation. Consumer choices are often based upon the best available information at the time with cyber hygiene, or the maintenance of a choice, unlikely to be a deciding factor unless the functionality is surpassed. As suggested earlier, at present the penalties that individuals and companies are subject to are not yet sufficient to cause behavioural change in market offerings.

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

Increased consumer focus on cyber security can substantially grow the market and further attract investors and investment in the industry. Government supported bodies such as AustCyber and the State based Cyber Security Innovation Nodes have played a key role in improving the scale, scope and quality of cyber security products and services, as well as being strong supporters of Australian based technology companies.

24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

People often refer to the need for good cyber hygiene which draws parallels to the Work Health and Safety (WHS) improvements over the last 30-40 years. During this time, improvements and changes to the WHS industry have largely been driven by an increase in the better capture of data for both incidents and near misses, as well as significant increases in sanctions (fines and even imprisonment) for organisations that fail to improve.

Cyber security as an industry is still in relative infancy, with many of the mandatory reporting schemes only coming into effect in the last 5 years as cyber security breaches have increased and consumers have demanded greater protection of their information. It is important that as this information continues to be gathered that Government adapts to a changing environment, identifies key areas of concern and implements sufficient legislation, frameworks and penalties for companies that don't maintain sufficient protections or meet the necessary standards.

25. Would you like to see cyber security features prioritised in products and services?

We believe this will largely depend on the industry or sector. Where security is valued the market will dictate what features, whether it be technical or compliance based, will be prioritised.

26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

The cyber threat environment will continue to change and we expect threat actors to stay ahead of the game based upon their own motivation, opportunities and capabilities. Many of the tactics, techniques and procedures used by adversaries can be mitigated through awareness and the establishment of cyber security standards. However, defending against cyber-attacks also needs to consider the human element which is most often exploited based upon human behaviour. Addressing these threats requires strategies to not only implement technical controls, but to also build an environment of trust with the wider Australian public that the data they share or hold online, is protected at all times.

It is important that the outcomes of the 2020 Cyber Security Strategy result in better outcomes for all interested parties, with clear deliverables that make Australia more resilient against cyber-attacks.