PO Box 6008
North Sydney, NSW 2060

15th of April 2023

RE: 2023 2030 AUSTRALIAN CYBER SECURITY STRATEGY- RESPONSE TO DISCUSSION PAPER

To Whom It May Concern:

The purpose of this letter is to provide a response to the discussion paper published earlier this year.

Mercury Information Security Services Pty Ltd (Mercury) is an established Australian cyber security practice. Founded in 2015, we have conducted in excess of 900 cyber security engagements for a range of clients including state and federal governments. Our organisation operates under the CREST scheme in the United Kingdom, and its staff are also certified as IRAP assessors. Its director, Edward Farrell, is a member of the ISC2 global board of directors, industry fellow at the Australian Defence Force Academy and an established cyber security researcher. The organisation has an established team of 15 consultants with collectively over 100 years of experience.

Our team has been consulted over the past few weeks to evaluate the strategy paper and consider the presented discussion questions. Attached to this letter is our response to the discussion paper. Mercury is pleased to provide its views on how we can work together to make Australia a world-leader in cyber security by 2030 and would welcome an opportunity to contribute further.

Should you have any questions or seek amplifying details, my contact details are below.

Regards,

Edward Farrell
Director | Principal Consultant

e: [redacted]
w: www.mercuryiss.com.au

Response to cyber security strategy discussion paper

An analysis of the industry state

The cybersecurity industry is at a state where an inverse incentive model exists, and technical skills and disciplines required to address the issues are valued less than the capacity to sell a product, service or maintain professional relationships that may not necessarily translate into a meaningful outcome. This has led to the following observations:

1. A neglect of technical disciplines; as it becomes easier to generate revenue purely through intermediary services in the cyber security; industry participants are incentivised to focus on the interdiction and management of a relationship or adherence to a bureaucratic mechanism as opposed to achieving an outcome.
2. As these intermediary skills can be quickly generated compared to technical skills, demand is artificially inflated in order to increase the volume of revenue to intermediary services even though its need may not exist, thus creating a skills shortage.
3. The artificially inflated demand has a risk of being met through underqualified supply, services that do not provide value for money or meet the requisite outcome, the subsequent mistakes of which need to be remediated through increased pressure on within the experienced market space which, as a result of the above issues, is no longer able to apply its services in a financially viable manner due to a deflation of what the market is willing to spend on cyber security. This in turn has a second order risk of undermining the trust and confidence of the industry and its capacity to operate, and sees an expanding industry that is not yielding an outcome.

Our analysis is based on the following qualified assessments:

1. Our statistics and current inputs are flawed, both in terms of economic necessity of products and services as well as the inference that the industry needs a large volume of personnel to address issues[1]. The qualified economic data to indicate demand and requisite personnel to address these concerns are not always properly qualified.
2. At one point in 2018, the number of recruiters in the industry relative to the roles and necessity was excessive[2].

Mercury is concerned that an inflated market exists that is not providing meaningful outcomes, and there is a risk that the current strategy and engagement by the government will only exacerbate this issue. The proposed time horizon, focus on strategy without in depth insights on technology or operational execution as well as the subjective hype may see a lackluster outcome. A theme central to our submission, is that those responsible for strategy development should critically analyse the “why” of the strategy as much as its influences, noting that simply throwing money or resources in an otherwise constrained environment may not address the issues that we as a country face.

[1] https://www.linkedin.com/pulse/why-im-weary-afrs-article-per-capita-report-cyber-skills-farrell
[2] https://www.linkedin.com/pulse/so-really-1-recruiter-every-4-practitioners-edward-farrell/

Standards and setting responsible conduct in cyberspace

Standards and setting responsible conduct in cyberspace are crucial because the internet has become a significant part of our daily lives. Cyberspace is increasingly being used to store sensitive information, communicate with others, and conduct business transactions. Without standards and responsible conduct, our digital landscape would be dysfunctional; standardisation of communications protocols has long formed the backbone of our digital infrastructure and methods of communication. Standards provide a framework for organizations to follow to ensure that they are taking the necessary steps to protect their systems and data. Setting responsible conduct in cyberspace ensures that users of the internet act ethically and protect themselves and others from harm.

Given the multiple, disparate standards, we can only express the concern that the government should not seek to reinvent the wheel and seek to leverage existing standards and practices. There are already many existing standards and practices that have been developed over the years which have been matured in the United States and Europe. We should leverage these standards and practices and build on them, rather than starting from scratch. By using existing standards, organizations can save time and resources and ensure that their standards are consistent with industry best practices and facilitate integration with the rest of the world. The introduction of wholly new approaches is encumbering, can lead to confusion and a lack of coherence in standards.

Simplification is critical when it comes to standards in cyberspace. Standards should be written in plain language so that they are easily understandable to a wide range of users. Complex standards can lead to confusion and misunderstandings, which can lead to a lack of clarity and confidence. Whilst . Simplified standards are also easier to implement, making it more likely that organisations will follow them.

Information security standards are not relevant to operational security and yet are consistently pushed as a solution. Information security standards are focused on protecting information from unauthorised access, use, disclosure, disruption, modification, or destruction. Operational security, on the other hand, is focused on protecting physical assets and processes from harm, ensuring availability and reliability. While there may be some overlap between information security and operational security, the two are distinct and require different approaches. The strategy that is under development should, as part of its consideration,

Standards for responsible disclosure

In 2016 and 2017, Mercury had attempted to conduct responsible disclosure for vulnerability research conducted on building management systems. The following outcomes were encountered:

1. Our first vendor contacted threatened legal action[3] and left building management systems in an insecure state for an extended period on our ongoing analysis.
2. The second vendor, an Australian company, was collaborative and had addressed risks throughout their client ecosystem within days. The vendor, in collaboration with the ACSC and their clients saw the need to address this vulnerability. This saw the securing of the affected systems which had included an RAAF base and a building management system at the Australian Nuclear Science and Technology Organization (ANSTO)[4].

Whilst the successful case was underpinned by collaboration and good faith on all sides, an opportunity exists to set standards and guidelines to enable responsible disclosure and support researchers, system owners and vendors in doing the right thing. We do not believe that an approach of forced disclosure is conducive to a positive risk culture; to the contrary a culture of collaboration and good will fostered by industry and supported by government, will yield a better outcome for society than the imposition of rules and regulations.

Communicating product security to stakeholders

In our experience, the process for effectively communicating risk and security to stakeholders is often ineffective and fails to delegate. Our experience with risk communication often sees the provision of sanitised versions of events after compromise or does not clearly communicate risk and management as a result of relying purely on a specific certification. Platforms like H1 and Bugcrowd often “allow” research performed against client environments to be published, but the ability to release the information is restricted or controlled by the person with the leak. Obviously this makes sense in certain situations, but sometimes it may mean there are vulnerabilities that go unreported or inappropriately fixed by vendors for an unknown period of time. It also prevents that knowledge from being shared within the industry, slowing down the rate that vulnerabilities in similar platforms may be identified and remediated thereby accelerating the remediation process. Mercury believes that the process of disclosure, as well as the communication of risk needs both a standardised approach as well as a process of community acceptance of risk.

[3] https://www.linkedin.com/pulse/why-i-couldnt-present-wahckon-edward-farrell

[4] https://www.abc.net.au/news/2017-05-06/software-bug-discovered-in-sensitive-government-systems/8501654

Standards for professional accreditation

Mercury's experience in the market and observations is that there is a need for professional accreditation and certification of industry professionals & organisations. Tradespeople, medical practitioners and lawyers all require some form of licensing and ongoing demonstrated learning. Similarly, financial institutions also require stringent regulation and licensing. Several years ago the representation could have been made that professional accreditation would stifle innovation and competition, however given the nature of the environment and the necessity highlighted in the discussion paper, this argument can be seen as moot.

The absence of certification and qualification has been the rise of unsuitable personnel for the delivery of cyber security services. Mercury has regularly encountered the outcomes of an unnamed individual (herein referred to as WUT) providing substandard services. The unnamed individual, who we suspect was the feature of a legal case *WUT v Victoria Police [2020] VSC 586*, has regularly represented themselves as a cyber security forensics expert with questionable qualifications over the past 7 years. In one such event in 2022, Mercury provided pro-bono support to a domestic violence victim who'd been charged $40,000 for cyber security investigative services by WUT to investigate a compromised phone, for which no technical services were conducted and the WUT had antagonised the perpetrator of the domestic violence. Whilst WUTs licence as a private investigator was suspended in 2020, no recourse to block WUT from providing cyber security services was available. The absence of such mechanisms presents a risk to the reputation of our industry and its capacity to police itself. By requiring accreditation, the risk of substandard or wholly inappropriate individuals within industry can be better managed.

Mercury has also regularly had to deal with managed security services providers that have provided substandard services. Of recent note, Mercury has regularly encountered service providers with overdeveloped sales staff and inadequate personnel for sustainment, which has featured as part of regular security evaluations[5]. Whilst a recent example has not been observed, the same concern should be extended to product liability, where cyber security products are not performing their intended function. Accreditation of service providers and verification of product providers claims will only serve to enhance the trust and confidence in services, however this should be tempered with a framework that ensures the process of accreditation is not simply a "tick and flick" exercise or prohibitive to limit new entrants into the market.

[5] https://www.youtube.com/watch?v=VMIUsnTtlm4
https://www.linkedin.com/pulse/how-respond-pen-testers-your-clients-network-open-letter-farrell/
https://www.linkedin.com/pulse/analysis-australian-mssp-soc-cyber-providers-edward-farrell/

Alternatives to education

Australia boasts a significant number of highly skilled practitioners, who do share some information and technical expertise with people trying to get into the industry. (Bsides sectalks et al) On the whole however, there are significant impacts that prevent true learning and cultivation of ideas. Whilst the knowledge of some things alone, aside from Web security there are often costly and physical barriers to entry, purchasing equipment, as well as access to a shared knowledge environment working on the same components makes this a difficult portion of industry to break into. It is however crucial to ensuring that more people have this knowledge would be to make available a space to test components in a business agnostic shared manner.

A multi layered education environment should be considered as part of our strategy to manage talent in industry and ensure workers, fit for purpose and developed in a timely fashion take place. This includes:

1. Academic education, such as undergraduate degrees. The utility of these degrees in analytic skills is exceptional, however often lacks hands on experience which sets graduates up for a longer period of learning.
2. Trade style education, where on the job training, consolidation and recognition of training takes place. This includes certification mechanisms such as CREST and ISC2.
3. Informal education and play style experiences, including competition based events, informal learning structures and social environments.

Mercury has fostered these approaches internally and advocates for their wider use across the industry. This includes Mercury's active participation in BSides, SecTalks, CREST, education providers and other events Australia wide.

Engagement of Commonwealth Government departments and agencies

The current method and process of engaging the commonwealth and the commercial environment is cumbersome, inefficient and dependent on time as a measurement for success. Time and materials billing for cybersecurity is problematic because it incentivises the cybersecurity provider to work slowly and inefficiently, in order to bill the client for more hours. This can lead to the client paying more for the same level of service than they would with a fixed-price contract. Additionally, with time and materials billing, the client bears the risk of unexpected costs if the project takes longer than expected or if the scope of the project expands. As the industry is dependent on rapid movement in order to neutralise threats, this process of delay prevents service providers from effectively addressing the problem. These issues can create an atmosphere of mistrust between the client and the service provider, which can ultimately harm the relationship and the success of the project. A fixed-price contract provides more transparency, predictability and an incentive for rapid movement.

Whilst information sharing from Commonwealth government departments and agencies is effective, there is more that can be done. Information sharing is crucial in the field of cybersecurity as it can help organisations detect, prevent, and respond to cyber threats quickly and efficiently. By sharing information about threats and attacks, organisations can leverage the collective knowledge and expertise of the cybersecurity community to improve their own security posture. This can include sharing information about the latest attack techniques, vulnerabilities, and indicators of compromise (IOCs). Sharing this information can help organizations stay ahead of potential threats and take proactive measures to mitigate risk. Additionally, information sharing can help organisations better understand the evolving threat landscape and adjust their security strategies accordingly. This can be especially important for smaller organizations that may not have the resources to keep up with the latest threat intelligence on their own. Ultimately, information sharing can be a powerful tool in the fight against cybercrime and can help organizations of all sizes stay protected in an increasingly complex threat environment. These activities are already underway within the ACSC, however wider sharing and enhanced mechanisms for sharing information should be considered.

In our experience, Government Departments internally and through regulation, have a focus on compliance over threat focused approaches to risk. Threat focused cybersecurity is better than compliance focused cybersecurity because it takes a proactive approach, focusing on identifying and mitigating actual threats rather than simply checking boxes to meet regulatory requirements. Compliance-focused cybersecurity often involves implementing a set of prescribed security measures to meet regulatory requirements, without considering whether those measures are the most effective way to mitigate actual threats or if they are in fact cost effective. In contrast, threat-focused cyber security involves continuously assessing the threat landscape, identifying potential vulnerabilities and threats, and implementing targeted security measures to mitigate those threats with a total view of the system or environment. By taking a threat-focused approach, organizations can better protect themselves against emerging threats and attacks, and adapt their security strategies as the threat landscape evolves, for which regulation may not be able to quickly adapt. This approach is especially important given the constantly changing nature of cyber threats, which can quickly outpace regulatory requirements. Ultimately, threat-focused cybersecurity is a more effective way to protect against cyber threats and ensure long-term security and resilience of our ecosystem.

Ransomware & email compromise: a question of economics

The question of ransomware and business email compromise is often raised within the community and has featured at several points in the Australian Governments discussion paper. This is often viewed with a technical lens as opposed to an economic one. In Brian Krebs book Spam nation (published 2015) which analyses the criminal environment between the late 1990's and 2015 identifies that the driver for crime was an absence of economic opportunity in Eastern Europe where most of the perpetrators existed. This same issue is becoming apparent with several, lower sophisticated attacks originating from Nigeria and emerging parts of the world, where economic conditions are more influential than the technology available. A technical driven approach we believe will not be as effective as an economic approach.

Economics present a more significant factor in cyber security events rather than technical prowess. In the early 90s, the motivation for a lot of cyber security events was financial; it was cheaper in terms of time and cost to exploit local phone exchanges rather than pay for dial up charges, the conditions of which were removed when internet service providers facilitated low cost lines for internet access. Bug bounties and economic opportunity globally have reduced several threat actors however the risk still remains of economic drivers, even smaller ones, facilitating exploitation . To offset threats, the capacity for prosecution such as the economic isolation of members of APT 1 and Sandworm serves as an alternative deterrent. By setting conditions internationally that facilitate positive interaction and economic enfranchisement, in concert with punishment and isolation for failing to adhere to rules and societal norms, the root causes that create threats to our cyber security environment can be drastically reduced.

Language, understanding and the lexicon: a side note

Mercury is also advocating the need for a common lexicon that disengages several terms and sets the conditions for the positive cultural environment noted above. This includes:

1. Reconsidering the phrase "ethical hacker." As ethics are subjective, the sustained use of this phrase may very well lead to the conclusion by an individual that a targeted attack on the Australian Government is ethical.
2. Terminology cataloging individuals as "white hat" and "black hat" "hackers". During a panel at Defcon 19 a highlighted point of cognitive dissonance was there is often the oversimplification of motive, means and intent which undermines our capacity to meaningfully deal with threats[6]. The augustinian framing of good and evil, and dismissal of anything in between is disingenuous, dismissive and will ultimately undermine our capacity to categorise threats and address them meaningfully.

Above all else, understanding the environment is critical and simply applying cliched terminology and concepts to the Australian Government's strategy will lead to a substandard outcome.

[6] https://jericho.blog/2011/08/06/whoever-fights-monsters-aaron-barr-anonymous-and-ourselves/