Submission No 13

INQUIRY INTO CYBERSECURITY

Organisation: Mercury Information Security Services Pty Ltd

Date Received: 18 September 2020

MERCURY
INFORMATION SECURITY SERVICES

Submission for the NSW Inquiry into Cybersecurity

Created for:	Portfolio Committee 1, NSW Parliament
Written by:	Edward Farrell
Version:	1.0
Date:	18th of September 2020

Table of contents

Document control

Version	Date	Author	Comments
0.1	15 September 2020	Edward Farrell	Originated
0.2	18 September 2020	Jared Smith	Peer Review
1.0	18 September 2020	Edward Farrell	Release

Overview

Mercury Information Security Services Pty Ltd (Mercury) is a Sydney based cybersecurity practice. Mercury has delivered more than 400 engagements to an array of clients including New South Wales (NSW) & Federal Government agencies, private sector clients and educational providers over the past five years.

As part of the NSW Portfolio Committee 1 (Premier and Finance) inquiry into, and report on, cybersecurity and digital information management in New South Wales, Mercury has provided the following submission in response to the terms of reference.

Our submission has focused on:

- Contractual arrangements between the NSW Government and providers of digital services and infrastructure. We have observed shortfalls in the validation of services delivered by these providers, and an underutilisation of contractual mechanisms to manage the shortfalls of service providers.
- The absence of reporting mechanisms within the NSW Government, which has allowed readily identifiable risks to remain present for an unnecessary length of time.
- The currently deregulated nature of the industry, which we argue poses a risk to NSW Government Agencies as well as NSW companies and individuals.

Throughout our submission, Mercury has provided its assessment of possible remediation activities, for which we would be available to discuss further with the members of the committee should the need arise.

We thank the committee for the opportunity to submit and look forward to the committee's findings.

Regards,

Edward Farrell
Director
Mercury Information Security Services

Observations

Assessment of contractual arrangements

The terms of reference solicited within the terms of reference submissions about:

> *Contractual arrangements between the NSW Government and providers of digital services and infrastructure, including:*
>
> *(i) Provisions relating to cybersecurity generally; and*
> *(ii) Reporting obligations and the monitoring of cybersecurity incidents;*

It is our assessment that whilst a good standard for monitoring & reporting of cybersecurity incidents has been observed in several organisations, shortfalls in monitoring and systems management as part of outsourced agreements have presented a significant risk to our customers.

This assessment has been informed by interactions with State and Federal agencies as well as the private sector. Over seventeen assessments conducted in the past year where a managed security provider was in place, our team was only detected three times in a manner that resulted in an adequate response. Additionally, ten providers were also identified not to have observed basic, common attacks that are commensurate with ransomware and other low tier threat actors.

The guidance that we have provided to clients relating to these matters has focused on service level agreement management, and ensuring that mechanisms are in place for the conduct cost recovery for nonperformance. To that end, we believe that an opportunity exists to hold providers of digital services and infrastructure to account and ensure that appropriate penalties are in place for failure of services.

The absence of reporting mechanisms within NSW Government

Mercury assesses that an absence of reporting and disclosure by members of the public to NSW Government agencies poses a significant risk, and undermines the availability of measurable data of security incidents.

During the conduct of an annual assessment and assurance activity with a client, One of our senior consultants had discovered a high-risk issue through digital reconnaissance that had affected a NSW Government agency.

We attempted to discover an individual to report to within the affected agency by our team and the client, no response was received and the risk remains present at the time of writing.

A similar issue was encountered between 2016 and 2018 with building management systems. Our own private research on building management systems identified that several facilities associated with the NSW Government were exposed to the internet and irregularly maintained. However we understand this has since been addressed.

Concerning both scenarios above, our team would be happy to provide detail separate to this submission.

The inefficiency to report on this matter presents a significant risk.

In addition to allowing risks to remain in place for an extended period, often the only course of action for professionals to gather attention to issue remediation is through public disclosure, which in turn undermines the ability of stakeholders to address identified issues appropriately.

Therefore, as part of our submission, we strongly recommend that the committee explores the availability of reporting or disclosure mechanisms, including allocation of responsibilities and response timeframes.

Any reporting or disclosure policies should be explicit as to what is reported as to what conditions with which such issues are detected to discourage active exploitation of NSW Government systems or other illicit behaviour.

The United States has recently mandated that all federal agencies enact a vulnerability disclosure policy by **March 2021**, for which a similar activity could be implemented in NSW[1].

[1] https://threatpost.com/u-s-agencies-vulnerability-disclosure-policies-march-2021/158913/

Accreditation and vetting of cybersecurity professionals & organisations

As part of Mercury's continuous improvement and quality assurance of its services, legal and operational liabilities alongside themes and risks have been observed within industry. Several areas of concern exist, namely:

- Methods and approaches to the delivery of services, including the delivery of offensive services that cause more harm than good.
- The qualification, location and vetting of cyber security practitioners.

There are an array of laws and regulations to consider when conducting cybersecurity services, including the Workplace Surveillance Act 2005 (NSW) and the The Surveillance Devices Act 2007 (NSW). These laws require the presence of an organisational policy for computer surveillance, and heavily regulate the employment of covert surveillance devices and data surveillance devices, including requisite permissions and notification periods leading into such activities, as well as the retention of recorded data. Some cyber security services, including aggressive cyber security assessments (red teams) incorporate surveillance on an organisations stakeholders, which legal advice we've received suggests this activity may fall within the *Commercial Agents and Private Inquiry Agents Act 2004 (NSW)*.

Whilst our team endeavours to comply with these laws during our assessment activities, it is our understanding that several other organisations have failed to factor in legal and ethical considerations into the delivery of services and advice. A deregulated cybersecurity advisory industry undermines the efficacy of assessment activities and can also lead to inappropriate guidance that is not backed by appropriate industry qualification. Furthermore, security advice provided, especially if physical security advice is provided (and fall under the *Security Industry Act 1997 (NSW))*, may pose a liability to the cyber security industry as well as the professionals providing such advice.

The intent of security legislation is to protect consumers from fraudulent, dangerous or questionable operators, and protect citizens from activities that infringe on their rights and wellbeing as well as assure the quality of services provided by reputable firms. Cyber security professionals and by extension IT staff are generally granted access to highly-secure digital environments and personal information. Unauthorised access or modification to this information can present a significant risk through insider threat scenarios which, as the global economy moves increasingly towards volatility, will become more likely.

Formal accreditation or recognition of industry competencies as part of procurement will enhance the professionalisation of the industry and reduce the likelihood of unscrupulous operators, as well as provide assurance that IT personnel are of good character and unlikely to perform actions that will have an adverse impact.

Having commenced this month an evaluation of cyber security firms in Australia and New Zealand, several themes and observations were made, namely:

- We've identified at least five firms purporting to be Australian cyber security organisations, with no in house capability contrary to their advertised services.
- Two firms present have offshored their entire capability, and have no locally trained personnel outside of management and sales staff.

In addition to the interjurisdictional risks of offshoring advisory, audit and monitoring activities, no requirement exists to conduct background checks or vetting of cyber security professionals or organisations. Whilst Mercury conducts background checks and vetting of competence of its current and prospective employees, an inconsistent approach across industry has been observed. A consistent approach and guidance to the qualification of cybersecurity professionals and organisations, including the use of formal accreditation through industry bodies will reduce the risks associated with offshoring cybersecurity services and the use of unqualified or unvetted cyber security professionals. A similar approach has been taken in Federal Government with the leveraging of security clearances; a NSW equivalent activity may also aid in the verification of cyber security professionals.

About Mercury

Mercury Information Security Services is a leading provider of information security services, advice and consulting in Australia.

Founded in 2015, Mercury provides sound and independent cybersecurity expertise across an array of domains. By customising our services to meet our clients' business requirements, we provide constructive and pragmatic security advice as trusted advisors.

For more information, visit their website or get in contact with them:

Website: www.mercuryiss.com.au
Twitter: twitter.com/mercuryiss
Email: info@mercuryiss.com.au