WATER SERVICES
ASSOCIATION OF AUSTRALIA

WSAA SUBMISSION

Australia's 2020 Cyber Security Strategy - a call for views

30 October 2019

Committee Secretariat

PO Box 6021
Parliament House
CANBERRA ACT 2600

SUBMISSION: Australia's 2020 Cyber Security Strategy - a call for views.

Adam Lovell

Executive Director

Water Services Association of Australia

Level 9, 420 George Street

SYDNEY NSW 2000

Ph: [redacted]

Email: [redacted]

I confirm that this submission can be made available in the public domain.

About WSAA

The Water Services Association of Australia (WSAA) is the peak body that supports the Australian urban water industry. Our members provide water and sewerage services to over 20 million customers in Australia and New Zealand and many of Australia's largest industrial and commercial enterprises. WSAA facilitates collaboration, knowledge sharing, networking and cooperation within the urban water industry. The collegiate approach of its members has led to industry wide advances to national water issues.

WSAA welcomes the opportunity to provide a submission to the Australia's 2020 Cyber Security Strategy - a call for views.

Summary of the water industry position

The water industry strongly supports the 2020 Cyber Security Strategy's focus and emphasis on the critical role water has to play in the economy. We would particularly welcome the opportunity to develop and deliver the strategy in partnership with the Australian Government. The industry supports greater education and awareness on cyber security issues. We also see the Australian Cyber Security Centre as a critical and currently underutilised resource, for dynamic risk awareness. The industry sees that clear standards for products and services would provide significant additional inroads into reducing the cyber security risk.

Water Industry cyber risk context

The Australian water industry provides essential water services using functional operating infrastructure, including; water sources (dams/groundwater/seawater) with treatment and distribution systems (pump stations, pipelines, treatment, tanks and reservoirs.) These systems utilise onsite digital information and operational technology resources, and offsite system control. All components of the system are separable with the majority of the schemes and systems including gravity and inline storage, geographically diverse multi-barrier treatment processes and therefore a malicious or internal systems disruptive event is unlikely to result in any extended loss of water services. Within this operating context the water sector utilise customer and asset operational databases to optimise the service delivery outcomes

The Australian water industry relies on local, national and overseas supply chains to deliver safe water services. These supply chains include manufacturing and logistic processes (e.g. chemicals, critical spares and database, service providers) and identifies that cyber risk vulnerabilities within these supply chains have the potential for a water service delivery disruptive event, beyond the capacity of the water industry to influence.

Liveable communities

The Australian water industry has a strong focus on water services to support liveable communities, and within this context the health and wellbeing of the general community is paramount. A community vulnerable to cyber safety risk could compromise these liveable community outcomes. Therefore the water industry strongly supports community wide cyber safety risk uplift programmes to support the health and wellbeing of the Australian community.

1.1 Responses to specific questions

1a What is the water industry view of the cyber threat environment?

That the cyber threat is increasing in the following ways:

- Increasing availability of low cost multi vector attack options, particularly through the dark web.
- The proliferation of attack options ranging from drones to auto bot software, along with increasing use of artificial intelligence options within threat vectors.
- An increasing reliance on digital applications and electronic systems for the management and delivery of water industry services, creating an increased exposure risk. Noting that this is to some extent countermanded by the use of accepted international protocols for device security, but which needs to be augmented by increased management training in addressing and responding to cyber threats.

1b What threats should the government be focusing on?

- Threats associated with large scale actors with hostile intent. Smaller scale actors are likely to have a localised impact which can be addressed at the local scale.
- Accrediting national IoT security protocols to minimise threat vectors associated with IoT and SCADA devices.
- Clarity on the preferred national standards and frameworks in relation to IoT and communications devices to minimise cyber security threats.
- Mapping of external supply chain risks to identify disruptive risks vectors, to enable the water sector to review the risks and contingency options.

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

The position put forward is a fair reflection of the current state. End users currently bear the sole cost for managing their online risk, and yet providers of goods and services relating to internet access often have a higher understanding of risks and mitigation options. The water industry would support greater education and awareness for supply chain vendors, and consumers, coupled with clarity on the most appropriate standards based risk mitigation options.

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

As an industry we would suggest that there is critical need for non-technical, informed risk based education, particularly of senior management in Australia. Some of the primary reasons for a lack of open disclosure to the Australian Cyber Security Centre are that there is a lack of clarity about its role and the consequences of reporting, due to the Government focus upon enforcement and regulation of critical infrastructure sectors, without informed and constructive, collaborative engagement. There is also a lack of corporate understanding of the benefit of rapid reporting and feedback on cyber events. Education would assist in addressing these barriers and help to ensure more effective and timely neutralisation of threats.

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

Consult to understand the nature of the threat and then seek to introduce and communicate reasoned standards or protocols to assist. Clarity on guidelines and appropriate risk based frameworks are the preferred next step after education and engagement. Legislation is an option, but should be used as a very last resort, as the water sector experience is that legislation and regulation delivers "minimal" and "minimum" compliance levels, which do not reflect the dynamic ally evolving cyber risk environment. The water sector has always positively responded to mature, efficient, risk based advice because this is an embedded fiduciary responsibility of all water sector entities

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

Through open and collaborative engagement and fostering collaboration between and within sectors. Clear and timely communication is critical. The quickest way to lose trust is to impose actions or obligations on organisations without sufficient engagement, avoiding due process or in a manner where the reason for the change in unknown, unclear or based on poor data.

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

The adoption or development of agreed national industry based standards, and communications with business (as the customers) as to reasonable contractual and service delivery levels.

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

The mental health and wellbeing of the Australian community is at measurable risk from relentless evolving cyber risk events, and therefore the water industry strongly supports cyber security (cyber safety) education programs within public and private education sectors at the earliest ages and reinforced within secondary and tertiary sectors. Stronger emphasis and support to developing risk awareness education and support programs to “CALD” and senior/s communities.

More emphasis (prominence and priority) should be given to supporting community cyber security (safety) risk awareness for home, and small to medium business, and also sectors not usually engaged by the national security strategies.

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

Efficient, and expedited production of acceptable “product” and service provider engagement standards for industry and business as “standards based reference points.”

Specific to “sector” industry risk awareness engagement programs.

Executive support-reference products focusing upon risk awareness and key positive points for organisational Cyber safety/security risk programs. Positive examples are from the TISN - Attorney Generals products where simple Executive checklists were provided and promoted,

The most productive approach is suggested to be through policy – not regulatory. Primarily the promotion of risk awareness and enabling joint support programs.

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

The preference is to keep the current functions within government to maintain and build trust. Commercial interests would be seen as having greater potential conflict of interest.

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

The current regulatory environment is weak and unclear in relation to the requirements on devices and cyber/digital services provided to consumers and the level of protection that is provided by each. Clear standards on protection levels would provide better assurance to consumers and allow appropriate selection of products that best meet consumer needs.

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

Introduction of relevant product and cyber/digital service security standards, coupled with effective consumer education. A campaign similar to food labelling is suggested as being an effective template.

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

Have clear standards that apply and ensure consumers are aware of the standards and what symbols/markings to look for that indicate compliance.

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

The introduction of open source accreditation programs against agreed industry standards and benchmarks.

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

Through an educated consumer base within industry and government, potentially assisted by frameworks and guidelines. Educated consumers will demand a higher quality of service, forcing the need for high quality cyber security professionals.

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

The water industry experience is that the insurance market to support cyber risk is rapidly evolving and maturing, and that there are existing national and international insurance products to support the sector requirements.

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

Through community and consumer education. Particularly around the impacts of behaviours and an understanding that the weakest link in cyber safety/security are people. Education involves training and education about how to avoid the inadvertent disclosure of sensitive information that could be used to compromise cyber security. This would include recognition of email and telephony based schemes.

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

Increase consumer awareness so that products have a higher level of cyber security, and consumers are less vulnerable to cyber scams. Provide constant risk awareness as risk vectors evolve. The community are educated and sensitised to online and nightly news weather forecasting and weather reports, and the water industry recommends that similar communication platforms are explored to deliver the cyber safety/security conditions on a daily or weekly basis.

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

Through risk awareness in a timely manner, and a connected, trusted network based around the Australian Cyber Security Centre.

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

IoT control and data feedback networks for the water sector. SCADA Networks for the water sector.

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

Options would include:

- A small fee charged with the sale of each consumer good or service.
- A voluntary fee paid by consumers.
- Businesses subscribe for services provided by the Australian Cyber Security Centre, or pay on a fee for service basis.

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

Constraints on information sharing centre around the following concerns, that:

- Information shared with government will not be securely maintained.
- The regulatory arms of government will access the data and use it to undertake enforcement or compliance action against businesses who provide data in good faith.
- Government could use the data to develop enforcement regulations that interfere with business operation and create a level of sovereign risk for businesses.

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

Almost totally. Improved awareness coupled with national agreement on preferred relevant standards would have a significant impact on cyber security outcomes.

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

It creates a market for products which are of high value through increased consumer awareness.

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

The Attorney Generals Department leadership of the TISN, using risk awareness and collaborative capability uplift, program support, generated positive change within the water sector. The advent of the current enforcement regime has measurably negatively mitigated against this previously positive engagement approach.

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

Yes, they should be clearly articulated in products and services, with accreditation and standards programs. However, this needs to be required in a manner similar to other consumer product disclosures to ensure comparability and transparency of claims to avoid confusion for the consumer i.e. the approach should be similar to labelling requirements for food products and done in a manner it avoids the confusion created in markets such as electricity and mobile phones.

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

- The water sector recommends that the operational and strategic delivery of the ACSC Joint Cyber Security Centre (JCSC), engagement strategy is reviewed, as currently the programs are manifestly directed towards technical risk. However organisational decisions are often made by others with non-technical backgrounds and organisational wide risk management responsibilities.
- The water sector also observes that the JCSC operating environment is no longer confidential, with many diverse industry representatives engaged within "the room". Therefore the open and honest communication and discussion of risk is compromised.