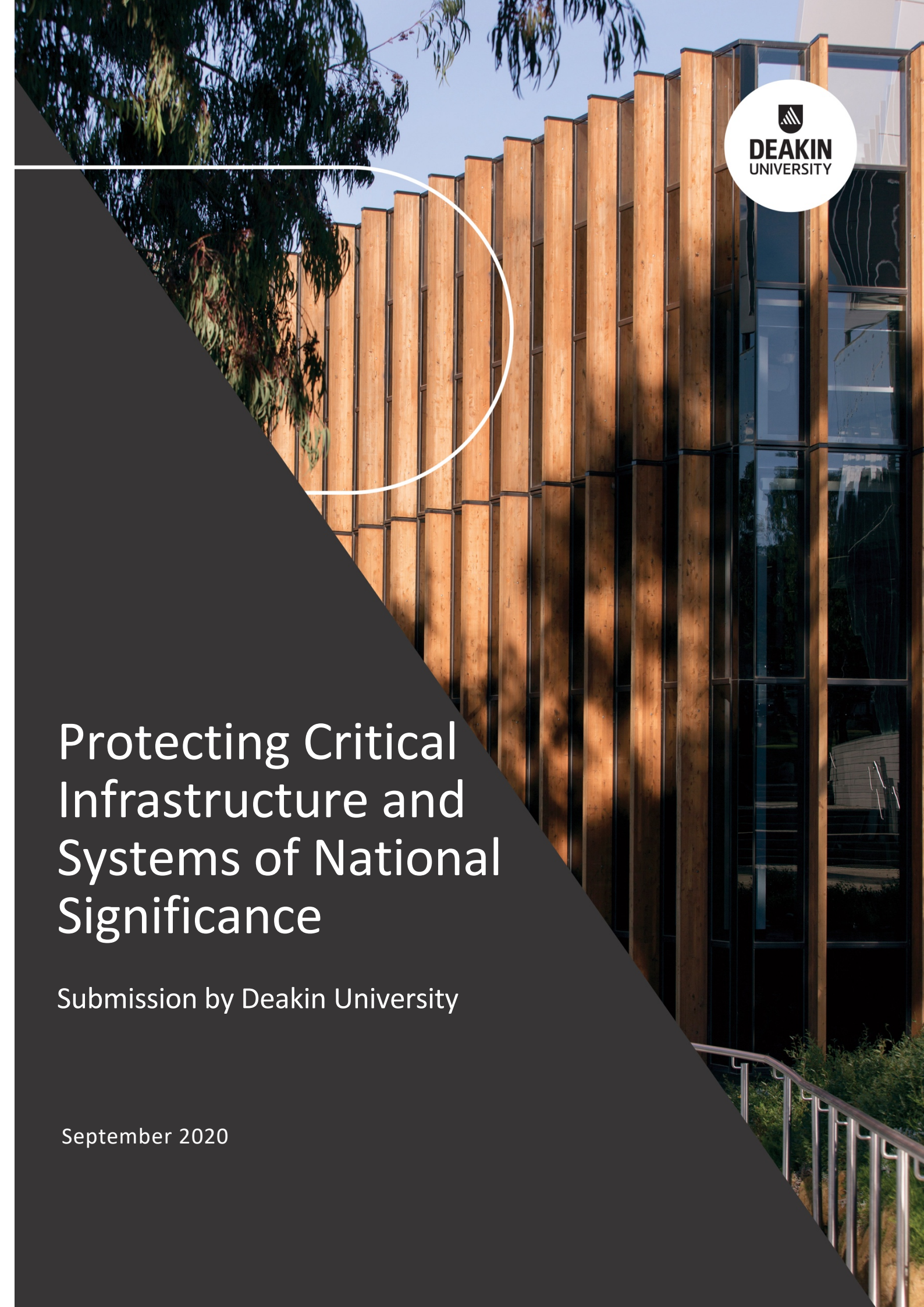

Protecting Critical Infrastructure and Systems of National Significance

Submission by Deakin University

September 2020

Protecting Critical Infrastructure and Systems of National Significance

Submission by Deakin University, September 2020

Introduction

Deakin University supports the Department of Home Affairs' intention to review and produce an enhanced framework to protect Australia's critical infrastructure from all hazards, including the dynamic and potentially catastrophic cascading threats enabled by cyber-attacks.

The approach of the one size does not fit all, balanced with objectives that provide a baseline of cyber, physical, personnel and supply chain protections across all sectors and taking into account the reality that there are sector specific differences in maturity and capability should be commended. The threat environment to Australia's economy has exponentially increased, particularly in light of COVID-19 and subsequent international pressures, further highlighting the necessity to uplift security of infrastructure and services Australians depend upon as the economy is digitally transformed. Caution needs to be taken to enable sectors previously not deemed critical to adjust to the new three layer definition of critical infrastructure and we welcome further clarification and refinement in consultation with industry and academia.

Since 2003, Deakin University has been a leader in cyber security research, education and innovation in Australia. Deakin has been awarded cyber security educator of the year for three consecutive years and has a range of undergraduate and postgraduate courses focused on cyber security, including combined undergraduate degrees with law and criminology. Deakin jointly with NTT (formally Dimension Data) supports Australia's only dedicated cyber security start-up accelerator, CyRise, now in its fourth year.

Deakin takes a holistic approach to cyber security, which includes Artificial Intelligence (AI), Information Technology (IT), data analytics, engineering, business and law, policy and regulation, psychology, humanities and health as these fields directly intersect with the future of our economy. This response is guided by the Deakin values of being excellent, ethical, inclusive and sustainable.

Deakin University makes three recommendations to the review committee:

- **Recommendation 1:** Establish an appropriate level committee to assess critical infrastructure providers for inclusion / removal from an evolving list at sub-category level of granularity.

- **Recommendation 2:** Consider interdependencies between organisations that may move some specific providers or suppliers into the critical infrastructure definition. In addition, there may be interdependencies between critical infrastructure providers that under specific circumstances may have the same level of societal impact as a failure of a system of national significance.

- **Recommendation 3:** Establish regulators or agencies to provide oversight to ensure compliance or adoption of potentially new frameworks / guidelines. These regulators must be selected on the basis of sufficient background knowledge on cyber security and business risk and must be sufficiently resourced to deal with the evolving complexities in each sector.

Deakin University's Response to the Review Questions

1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?

The sectors that have been listed in the paper would require further refinement in terms of their scope in the industry landscape of Australia. Having a general list of sectors under a common critical infrastructure definition may encumber the process of categorisation of industry based on their levels of criticality. Understandably, a lot of critical sectors do exist in the Australian context. Some areas of the manufacturing sector could be classified as critical infrastructure, however, the sector as a whole may not necessarily have a direct impact on the nations' economy, security and sovereignty. Certain manufacturers who provide specific services, products or are deeply interconnected in supply chains (i.e. key risk dependency) with other key sectors (e.g. PPE manufacturers in times of pandemics, defence). Having a range of sub-categories under each of the sectors defined, may be a better way of accurately presenting the Government's framework for safeguarding critical infrastructures. An appropriate Government Committee could be convened to include critical infrastructures and sub-sectors into an evolving list.

2. Do you think current definition of critical infrastructure is still fit for purpose?

Critical infrastructures are generally defined based around their degree of criticality to a nation's security, economy and sovereignty. Given the comprehensive scope of a critical infrastructure in terms of its impacts on our daily lives, expanding the definition to become: '…economic wellbeing of the nation, or affect Australia's ability to conduct national defence, sustain citizen livelihoods and ensure national security, would be a more accurate portrayal of a critical infrastructure.

3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

Critical entities can be identified and prioritised through a formal study of resources that belong to an entity, their levels of classification and the outcomes of a risk assessment procedure which is conducted to analyse the consequences of resource compromise.

4. What are the common threats you routinely prepare for and those you have faced/ experienced as a business?

Some of the common threats faced by industry and that require routine preparedness include:

- business disruption
- unintended data disclosure including data theft, intellectual property loss, data held for ransom (ransomware), contract cheating (education industry), and online fraud
- compromise of safety systems – fatality and injury, environmental damage/injury
- diversion of product – supply chain compromise, product diverted to a non-legitimate customer, money diversion (banks)
- misinformation including social cohesion.

Despite this, many of these threats do not have a direct impact on the sovereignty, economy and security of the country, depending upon the sector in question. Cybercrime can be perpetrated and concealed as white-collar crime, so the threat landscape is very fluid in cyber space, but can be expanded to comprise all interdependencies both from within and outside the technological (cyber) space.

5. How should criticality be assessed to ensure the most important entities are covered by the framework?

Interdependency between the entities, would cause a knock-on/domino effect across various other sectors of industry. In addition, the threats as enumerated in (4) above can help assess the criticality of entities and their levels of impact when these entities are incapacitated from continuing to deliver cyber security to safeguard national security, economy and sovereignty.

Criticality ought to be assessed in terms of immediate and long-term impacts of the entities on sustained critical infrastructure activities. Consequently, an impact table when formalised for each of the identified entities, would help ascertain that the entities are duly categorised in terms of their impact to the nation, when they are subject to a cyber-attack. The type of attack and the consequences would help inform the impact table. For example, an attack on a single supermarket versus an attack on a key service provider which limits the ability of all supermarkets to function and provide goods and services to the public and businesses.

6. Which entities would you expect to be owners and operators of systems of national significance?

The current draft of the proposed Government Framework for Protecting Critical Infrastructures, is vague in definition of 'systems of national significance.' Without a proper understanding of what comprises such systems, by definition, it would be hard to analyse and enumerate the list of potential owners and operators of such systems. An entity can be owned by the sector players, e.g., a gas service provider would be the owner of the gas distribution network, and the operator can be the contractor responsible for system functionality and sustenance.

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

The TISN model can certainly be revised so as to do away with its current method of operation comprising passive activity through moderation and administration of discussion forums, that are built around little to no structure i.e. a lack of agenda on the cards encumbers the ability of the TISN to deliver to its objective of bringing together the Government and industry and to share intelligence information that would help the industry better safeguard their entities/assets against the evolving cyber threat landscape.

The TISN can be organised into value streams with a vision to realise community outcomes, from a national objectives point of view and to also tie in with the Critical Infrastructure Resilience Strategy, by accurately mapping interdependencies amongst the various entities and other players.

8. What might this new TISN model look like, and what entities should be included?

Expectations are needed to bring more focus and to help critical infrastructure sectors. The new TISN model can certainly work to a properly defined agenda from the Government, and closely with industry, in order to be able to share intelligence data with them and to help the industry safeguard their assets/entities from cyber threats. The current TISN model has been ineffective in guiding the industry on the advisory for cyber security, considering the evolving intelligence around cyber threats, that the Government can certainly share with selected members of a given critical infrastructure sector.

The paper specifies that new requirements will build on and do not duplicate existing regulatory frameworks (Page 12). Some sectors that are mentioned in this paper that are critical infrastructure (page 3), such as the private healthcare sector, are currently not in scope of the security of Critical Infrastructure Act 2018 and currently have minimal regulatory requirements or oversight with regards to security.

When considering the proposed framework (page 13), such sectors would potentially miss out on the opportunity to improve security maturity as part of this initiative, given it appears they would potentially not be subject to some of the key elements of the proposed framework, such as the Positive Security Obligations. We need to make sure that similar sectors not already defined in the security of Critical Infrastructure Act 2018 are carefully considered and given the right considerations in the best interest of overall critical infrastructure protection and protection of our nation.

9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

Sector interdependence is not common. Banking for instance, wherein the four major banks can collectively operate to defend against a common and sustained cyber threat. The framework ought to provide the right interface to facilitate sharing of cross sector intelligence data (government to industry), that will have a common impact across the various sectors. Additionally, coordination between various entities of the sectors and with the media can be supported through engaged directions that can be provided by the Government. Consequently, fake news can be

countered successfully by the sectors. The Government can also help industry simulate cyber-attacks to ascertain that systems are continuously tested to operate per requirements. Good training on cyber threat handing and incident response can also be an essential support task that the Government can customise for the various critical infrastructure sectors.

10. Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

The general list of principles is broad enough to cover security risk holistically. However, details on how these principles can be customised for specific critical infrastructures, has not been presented in the paper. It also begs the question as to what an 'entity' is? And how a defined entity fits into these four principles from a risk management perspective? We can work out a tick and flick approach, as is the case for a lot of industries out there, however, without a proper advisory in place, industry would be left in the dark on what level of governance comprising support can be provided to them for handling the core cyber threats as enumerated in (4) above.

11. Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

There ought to be a clear mandate on board level involvement in threat management, which can be posed as a security requirement for the industry. Additionally, industry-specific requirements can help the industry and relevant regulators to better comprehend sectoral needs and how best the Government will fit into the picture, when it comes to supporting businesses in the event of cyber-attacks, with adequacy in provisioned support.

With bureaucratic procedures in place, potential slower acts of responses to imminent threats can jeopardise business operations and could also encumber the response process. It is therefore essential for the Government to clearly identify the security requirements that are sector-specific, in order to ascertain that the most appropriate level and type of support is provisioned during crisis times.

12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

Not all organisations would be in a state to meet these principles from day one. Even within a common Critical Infrastructure sector, not all the service providers would be on the same page when it comes to cyber security principles, adherence thereof, risk management strategies and readiness to counter zero-day attacks. Consequently, a serious disparity may be witnessed in criteria and readiness to follow these principles when the proposed framework is introduced at a sector level across the country's critical infrastructures. A question that remains unanswered in this paper is: gauging the principles-based approach, what role would the Government have in provisioning and sustaining support for the industry to enable them to meet these principles?

13. What costs would organisations take on to meet these new obligations?

Some of the attributed costs for organisations to be able to meet these obligations would comprise compliance activities and compliance headcount. Additionally, upskilling of personnel would be essential to enable them to work closely with regulators and the Government, and to define a process to follow for risk management and emergency response.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

Currently, security obligations lie within certification and regular auditing of security devices and controls in a corporate environment. Such obligations are specific to the sector in question and do have associated costs in terms of human capital, resourcing for risk management and training.

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?

Oversight arrangements generally comprise a statutory authority, Commonwealth ombudsman, an inspector general in charge of national intelligence and security and a royal commission. The regulatory model can better serve the framework through a clear definition of how it would fit into an ongoing industry sector system design and maintenance through compliance with national and international standards. Such a setup would be heavily dependent on the sector and would entail a clear demarcation of responsibilities in terms of compliance adapting in a two-pronged manner; Commonwealth at one end and adherence standards at another.

16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

The choice of regulators would directly impact the success of the industry to meet their obligation, as the regulatory authority may not be skilled and knowledgeable for a given sector. Regulators ought to work on input and output signals provided by the relevant stakeholders. These can be derived from threat intelligence received from the Government, to foster a better industry-government regulatory setup. Additionally, a policy and procedure around technology stacks, threat outcome management, budget management, costs relating to system setup and redefinition to adapt to the new regulatory process are to be considered. The regulators can have a deeper insight only if they are operating in proportion to resource allocation that pre-exists within the current industry systems. Such guidance can be better adapted if it is defined and placed in order beforehand.

17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

Without a proper definition of the expectations from industry from the overall Government strategy for protecting critical infrastructures, which seems to be missing from the paper, it is hard to gauge the type and level of commitment required of a regulator. Consequently, we are unable to provide accurate advice on who the security-related regulator ought to be?

Some general limitations of the role would be witnessed through a lack of precise definitions on organisational resilience, comparison between compliance and adaptiveness, immediate and long term threat impacts and the level of a sector's readiness to enable a process-driven approach to complex problem solving.

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

- Types of government threat intelligence data that can expect to receive.
- Level of commitment of the liaison security personnel of the sector/industry.
- Expected outcomes of a regulatory exercise.
- Frequency of intervention on a threat-free day.
- Type of intervention required during a national emergency.
- Cost factors for both the Government and industry to handle a crisis situation emerging through a cyber-attack.

19. How can Government better support critical infrastructure in managing their security risks?

Industry is long overdue for a proper framework to be put in place to be able to receive realistic, valuable and time-efficient threat intelligence from the Government. Such data would enable the industry in general and specifically those associated with critical infrastructures to be able to better defend their systems and to help safeguard the national sovereignty, economy and overall security. Within a strategic context, if the industry is advised by the

Government on what is important in terms of risks posed and the accompanying advisory on how best to manage the same, it will be beneficial to all stakeholders.

20. In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

Background checks as conducted through AusCheck as well as the ASIO approach for mitigating the risk of insider threats is limited to insider (within boundary) threats. Moreover, cyber professionals involved in the scheme may not be accredited to carry out a certain aspect of risk management. Hence a mere background check must not be sufficient to certify an individual's skill to undertake such a task. The scheme will have to be expanded to be able to cover a broader range of cyber threats, including those emerging from nation-state sponsors of cyber-attacks against the nation's critical infrastructure. A policies-based framework will be a beneficial reference for the industry and would also provide the sector with guidance on how a national-level security assessment can help leverage existing security controls to better safeguard critical infrastructures against the ever-evolving threat landscape. A consistent approach across all sectors in terms of reference Government frameworks for risk management would be a good way forward.

21. Do you have any other comments you would like to make regarding the PSO?

A proper set of definitions around the four principle-based outcomes would certainly prove to be beneficial to the industry. Now, the directives and actions entailing through the proposed Government framework presented in the paper seem to be drawn up from existing frameworks and acts on protection of critical infrastructures of the nation. Moreover, without a proper definition in place for the various types and categories of entities in the framework, the onus of responsibility in the event of a cyber-attack, cannot be imposed on the industry; justification of such a procedure may be weak by definition.

22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

Actionable threat intelligence is good for the industry. However, the question that may be posed here is: whether the Government will be carrying out vulnerability scans for the defined entities of the framework? In such a case, they will be executing an action that can be construed to be at odds with an industry-first approach to risk management. Moreover, will the Government be undertaking vulnerability scans and incident response actions that will be different from the existing security vendors undertake their business?

Cyber security skills-based training and capacity development is also a suggested preparatory activity for helping the Government proactively identify and remediate cyber vulnerabilities.

23. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?

- Threat intelligence; national and international levels.
- Response guidelines from other governments to advanced and persistent threats.
- Level of support that the Government will be providing, technical specifications, level of Government involvement.

The benefits of such information sharing would be realised through a sustained, consistent and effective risk management process in place for all critical infrastructure sectors of the nation. Moreover, the ability of the industry to support the Government can be at its maximum benefit if the threat intelligence data shared by the Government is current and specific to the various sectors.

24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

Universities face the threat of external actors attempting to steal intellectual property from researchers. The threat picture contribution from a university perspective can comprise past incidents that may have had consequences to national security and sovereignty. Cost implications for sharing such intelligence would be reliant upon the following factors: hours of effort required to retrieve data from cloud repositories, policy definition efforts to safeguard from data leakage, identification of stakeholders for the data being analysed.

25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

Methods for identification of vulnerabilities at the perimeter of critical networks could include: layered security (defence in depth), policy definitions and policy revision frequencies, board level involvement into cyber security decision making, dedicated security personnel for architecting security at platform, system and end-user levels, maintaining security and educating users of the threat landscape.

26. What are the barriers to owners and operators acting on information alerts from Government?

- Lack of clarity in guidance for security received from the Government.
- Lack of guidance on risk management at sector level.
- Lack of threat intelligence data shared by the Government with the industry.
- Lack of a proper structure for entity to regulator to Government risk management for critical infrastructures.

27. What information would you like to see included in playbooks? Are there any barriers to codeveloping playbooks with Government?

Threat intelligence data from the Government, possibly obfuscated to reduce the risk of unwanted data sharing at the incorrect classification levels.

Sector-wise definitions of situational awareness and cyber security drills may vary significantly and may thus encumber the process of codeveloping a playbook.

28. What safeguards or assurances would you expect to see for information provided to Government?

- Policy and procedure for secure transfer of information from the industry to the Government.
- Policy and procedure for secure storage and processing of the information.
- Details on level of involvement of the regulators and the Government liaison officers for assessment of the information provided.

29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

If Australia was under an active cyber-attack that is affecting the national security, economy and sovereignty, then the critical infrastructure sector being compromised can be directly approached and requisite actions to mitigate the effects of the attack can be taken. Actions can include:

- disconnection of the ICT network with the rest of the world
- deployment of cyber troops for handling the incident in hand and to reduce the risks of spilling over of the attack into other territory in cyber space.
- advisory on media engagement given to the industry.

30. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

It would be good practice to receive advice from a number of relevant agencies, including the Department of Defence, ASIO, Australian Signals Directorate and the Federal Attorney General's department to declare a critical infrastructure emergency.

31. Who should oversee the Government's use of these powers?

The Government's use of these powers should be overseen by a Statutory authority including a Commonwealth Ombudsman, and the Inspector General.

32. If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?

Actions would certainly be more focussed and impactful if they are specified for threat actors based on their geo-locations in cyber space. The ASD/Defence offensive cyber security capabilities can come in handy to disrupt a perpetrator within national borders. A comprehensive external threat handling strategy must be defined by the Government and included as part of any framework for protecting critical infrastructures.

33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

Liability protections for officers involved in emergency actions are both useful and essential. The industry should not have the legal authority to be able to do so. Having said that, critical infrastructure operators have control over their networks, and ought to be legally protected from any implications of failed outcomes from an adversary disruption exercise. Operators and owners of a system or a network would not be requiring any legal protection, as they will be carrying out their routine jobs. External powers including the Government intervening to disrupt a threatening event would require legal analysis to define bestowment of holistic legal protection for emergency action officers. However, they should not be afforded protection for wilful damage or negligence through poor preparation and poor risk management practices.

34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?

- A policy on accountability of officers involved in threat disruption activities.
- Proper measures for data logging.
- Clear definitions of powers of entities, regulators, and Government personnel in charge of critical infrastructure risk management.
- Clear explanation on minimum risk management criteria including policy, personnel and controls that are deemed as essential for sustained operation of critical infrastructures, safeguarding the national's security, economy and sovereignty.

35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

The risks to the industry through such an approach are as follows:

- Compromise of intellectual property that was inadvertently accessed by officials (in-charge) of attempting to disrupt an ongoing cyber-attack.
- Lack of threat intelligence leading to inconsistent or ineffective risk management across the industries.
- Lack of assistance for the industry to help them assess their security maturity levels.

- Unintended data disclosure including data theft, intellectual property loss, data held for ransom (ransomware), contract cheating (education industry) and online fraud.
- Compromise of safety systems – fatality and injury, environmental damage/injury
- Diversion of product – supply chain compromise, product diverted to a non-legitimate customer, money diversion (banks).
- Misinformation including social cohesion.

36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

The roles and responsibilities as outlined in this paper are not very clearly defined. We are unsure what an entity would be for a given industry sector and how a regulator would fit into the bigger picture of things, whilst attempting to provision Government support to help protect critical infrastructures. Consequently, it is difficult to gauge by how much and to what extent the involvement of the private sector in managing the risk would change, through such proposed increase in Government involvement for risk containment.

Contributors

Wouter Veugelen, Chief Information Security Officer, Health Sector

Jamie Rossato, Vice President IT and Cybersecurity, Orica

Professor Robin Ram Mohan Doss, Director of Research, CSRI Deakin University

Professor Peter Eklund, Research Division Leader, CSRI Deakin University

Fadi Jafari, Information Security and Risk Manager, eSolutions Deakin University

Abbas Kudrati, Chief Cybersecurity Advisor, Microsoft Corporation

Industry Professor Min Livanidis, School of Information Technology, Deakin University

Dr Adrian Panow, Director, Deakin Energy

Dr Hermione Parsons, Director Deakin Centre for Supply Chain and Logistics (CSCL), Deakin University

Garry Bentlin, Chief Security Officer, TransGrid

Professor David Fairman, Chief Security Officer, Data and Cloud Sector

Richard Heron, Chief Information Security Officer, Melbourne Water

Catherine Buhler, Chief Information Security Officer, Energy Sector

Eshan Dissanayake, Head of Digital Security, Food and Security Sector

Dr Zubair Baig, Research Division Leader CSRI, Deakin University

Damien Manuel, Director Deakin Centre for Cyber Security Research and Innovation (CSRI), Deakin University