



OCSC

Oceania Cyber Security Centre

Protecting Critical Infrastructure and Systems of National Significance Submission

September 2020



The OCSC: Defining the new frontier

Protecting what is critical to Australia's sovereignty requires looking beyond our own borders to include our neighbours and partners. Setting clear parameters on what defines critical infrastructure and what constitutes effective national security governance must be considered at a national and international level.

The Oceania Cyber Security Centre (OCSC) was established at the end of 2016 as a collaboration between eight Victorian Universities and the State Government of Victoria. The Centre provides a platform for Industry-led cybersecurity research in addition to delivering the University of Oxford Cybersecurity Capacity Maturity Model for Nations (CMM). To date, the OCSC has successfully led six CMM review missions with neighbouring nations and international partners in the Oceania region.

The OCSC works with international partners such as the International Telecommunication Union (ITU), Asia Pacific Network Information Centre (APNIC), Asia-Pacific Telecommunity (APT), World Bank and the Global Forum on Cyber Expertise (GFCE). We work at the forefront of research to strengthen cybersecurity capacity and build contextualised resilience, exploring questions of what works, what doesn't work and why.

Our expertise across cybersecurity is all-encompassing, rich and diverse. It includes expertise on:

- policy and strategy;
- culture;
- education and training;
- law and regulation;
- governance and structure; and
- incident response and technical controls to protect information and intellectual property (IP).

The intention of the current consultation exercise – 'Protecting Critical Infrastructure and Systems of National Significance' – is to introduce an enhanced regulatory framework, building on existing requirements under the Security of Critical Infrastructure Act 2018 (the Act). A key focus as outlined in the August 2020 Consultation Paper is the intention of Government to work in partnership with critical infrastructure entities to ensure the proposed new requirements build on and do not duplicate existing regulatory frameworks.

Our submission provides specifically researched and referenced examples of where frameworks, definitional aspects and enhance information sharing could assist the government to achieve this objective. A starting point as articulated in our response to Question 24 would be to conduct a Cybersecurity Capacity Maturity Model for Nations (CMM) review for Australia to assess the technical and non-technical dimensions of Australia's critical infrastructure assets related to cybersecurity, with a view to build an evidence base, independent from government and industry, around best-practice responses to advanced and persistent threats. This would add to the intentions of the Critical Infrastructure Program for Modelling and Analysis (CIPMA) and would provide the necessary research, threat, data and risk analysis required to provide a more detailed depiction of the threat environment and subsequently contribute to better policy outcomes.



A National Framework for the Governance of Critical Infrastructure Protection

The critical infrastructure ecosystem is complex, involving multiple stakeholders with competing priorities and operational alignments, with multiple interdependencies across organisations and national and international borders.

Regulation and compliance alone will not be enough to move away from old ways of working, aiming for a tick in the box or installing the machine that goes ping. Real change will require all stakeholders to engage in understanding risk and be supported to effectively manage risk as an ongoing activity in response to the current and changing environment.

There is a definite need for the Australian Government to define the roles and responsibilities of key actors and stakeholders in critical infrastructure protection (CIP) and a need for a multifaceted operating environment that makes sense.

We need a formal structure through which we can define and monitor CIP objectives taking into account new dimensions that encompass the CIP horizon of additional complexity. These complex dimensions can be elaborated by indicating the value of intangible entities such as intellectual property (IP) and human resources.

As the CIP environment continues to evolve in its complexity, finding the balance in supporting innovation in a resilient environment is key. National appropriate resourcing, sustained funding and transparency around what support will be available to organisations, oversight of powers and accountability will be vital in the delivery of successful change even if the how must remain confidential. There is a real need to step away from recycled practices, invest in a strategic roadmap and effective execution that includes Australia's incredible expert pool and research talent.

Q1. 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)?

What we consider as critical has changed significantly in the shift from an industrial economy to a knowledge-based economy. The pivot at pace in response to COVID-19 has highlighted existing concerns around supply chain management and accelerated digital transformation. The new normal may make it easier to access services; create new ways of working; trade with others; learn new skills; and connect people in times of social distancing. However, digital transformation at pace often relies on cloud-based digital platforms that store or process data outside Australia.

Through public consultation, there is a need for a new definition of critical infrastructure that should consider digital platforms and knowledge assets to look at ways of tackling intellectual property theft, while considering different levels of criticality to scale controls accordingly. Though care must be taken to avoid an all-encompassing definition which loses focus on protecting what is important, stifles innovation and limits the ability of organisations to compete on a global scale through wide reaching regulation.

It will be important to have a deeper consultation to develop definitions with clear examples of organisations, people, processes and teams that are in scope, including more details of proposed controls, enabling stakeholders to provide informed feedback. Any obligations that come out of a broadening of the definition of what is critical must come with sufficient support to enable entities affected to respond effectively. Sufficient funding and resourcing will be important to avoid reinforcing the existing culture of compliance to meet minimum standards that pass audit before returning to business as usual, when a culture of ongoing engagement in effective risk management is the desired outcome.

Minimum standards should be considered in the context of levels of criticality to avoid the risk of lowering existing standards in higher maturity sectors.

The inclusion of data and cloud is complex. Most providers are not Australian businesses and data is stored offshore. There is a need for a deeper discussion of data and cloud to explore what is in scope and what is not. Special care will be required to work with cloud providers to develop and negotiate Service-Level Agreements that protect related infrastructure and information assets.



Q2. Do you think the current definition of Critical Infrastructure is still fit for purpose?

As Australia transitions from an industrial economy to a knowledge economy, the notion of what is 'critical' must be revisited. Although digitalization has transformed the way Australians and Australian organisations operate, it has also had the adverse effect of increasing our vulnerability to cyber-attack and disruption. In particular, data, information and knowledge are collectively the oil that fuels our productivity and are now essential to our way of life.

We believe that critical infrastructure must now include those stockpiles of valuable and competitively sensitive knowledge that drive our innovation. In fact it is this very innovation that has been the target of numerous cyber-attacks from strategically-motivated and state-based actors. Our research on Advanced Persistent Threats may help to tackle this problem as it profiles cyber attackers that have been targeting and stealing intellectual property for competitive advantage (Ahmad et al. 2019).

Theft of intellectual property has been a particular concern in Australia and widely reported in the media. In 2013, the ABC documentary series Four Corners claimed that foreign hackers stole 'national security secrets and vital business information' from Australian organisations such as BHP Billiton, Rio Tinto, Fortescue Metals Group, BlueScope Steel, and Codan (Fowler & O'Brien, 2013) but with much of this theft remaining confidential has made it difficult to measure the extent of the problem. However, the release of the national Cyber Security Review followed by the Cyber Security Strategy at the end of 2015 points to 'cyber-enabled intellectual property theft' as an important and urgent national security problem.

We also believe that the definition of critical infrastructure must be revised to include the 'digital platforms' that Australians rely upon to work, trade, communicate, and seek information. In fact the use of digital platforms has profoundly changed the way our government functions and interacts and delivers services to Australians. Digital platforms are more than just information technologies, they provide functionality and experiences resulting from integration with organisational processes as well. Further, the complexity of digital platforms and their inherent distributed nature introduces cross-border dependencies (e.g. overseas stores of big data and cloud services that are essential to digital platforms) and exposes Australia to neighbouring actions and their impact.

Our research shows that cyber threat actors have engaged in campaigns of information influence ranging from attempts to compromise these critical digital platforms (e.g. election voting systems, communications platforms) to spreading false propaganda and 'fake news' (Desouza et al., 2020).

Q3. 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?

There are several factors in addition to interdependencies that may impact critical infrastructure. These factors relate to issues linked to the physical and technology aspects of infrastructure. For example, where assets are located and the technology they use. These issues gain additional complexity when we consider the unique aspects of Australia. For example, our federated model of government means that a single critical infrastructure, such as a telecommunications network, could have cross border dependencies across the states and territories within Australia and even outside of Australia.

Australia now has a situation where several states are developing their own state based critical infrastructure policies and in theory define their own critical infrastructure. This could result in conflicting governance between State and Federal legislative parameters. For example, in Victoria the water critical infrastructure sector could be directed by Home Affairs or by the Victorian Auditor General to make security changes, with different security advice being offered. Thus critical infrastructure owners may receive conflicting advice and be unsure which to follow.

A considerable portion of Australia's critical infrastructures is owned and operated by private organisations. Given the primary objective of private organisations is service availability, the level of resourcing is adequate for low level incidents such as those caused by accidental or natural hazards. This means that resourcing may not be enough for protection against organised and sophisticated attacks. Therefore, under-resourcing of coordination and protection capabilities among private organisations creates new risks such as interdependencies within and between organisations due to poor or inadequate coordination and management of teams and individuals.

Australia also has the issue that some critical infrastructure owner organisations are non-Australian and are owned by international organisations, for example the Victorian power sector. This causes issues as overseas organisations may not be interested in improving cybersecurity in Australia as they have competing priorities between the overseas organisational objectives and the Australian Government objectives. This could also mean that international organisations may not be able to scale their emergency responses or respond to the cybersecurity requirements of the Australian Government.

Due to the COVID-19 situation, we may also have a situation that private critical infrastructure organisations may be forced to reduce costs meaning they may consider outsourcing and offshoring of key cyber services to reduce costs which could have a potential security risk for Australia.





Q4. What are the common threats you routinely prepare for and those you have faced/experienced as a business?

The cyber threat landscape is dynamic, complex and industry dependent. Week to month the nature and complexity of the threat changes. One such example is Ransomware. Ransomware are changing their behaviours to cause maximum harm and to evade detection. Online service delivery by critical infrastructure has expanded the attack surface area significantly and has attracted the attention of organised criminals to exploit vulnerabilities in integrated critical infrastructure systems. Ransomware attackers also exploit the trust of the victims, as it is common understanding that ransom payments may not restore the access to information systems fully. Sophisticated attackers are using trust to make it more attractive to pay the ransom than not.

State Nations and cyber criminals are actively mapping critical infrastructure architectures to plan attacks, mounting ransomware attacks to degrade operations, organising human assisted insider attacks and changing system configurations remotely for malfunctioning.

OCSC sees a rapid militarisation of the digital environment due to the release of military-grade cyber weaponry in the wild. For example, Shadow Brokers released an arsenal of NSA high-tech weaponry into the wild back in 2017. Among these was 'Eternal Blue' which was subsequently used in ransomware attacks against a number of cities and local councils. The point here is that mid-level threat actors are being elevated to the same status as nation-state threat actors thereby creating a fundamental asymmetry between threat actors and defending organisations. Easy threats and harder threats thinking needs to change because of the militarisation of the weaponry as the shift will continue in sophistication. Organisations that are less able to protect themselves will need assistance to defend against sophisticated actors.

Q5. How should criticality be assessed to ensure the most important entities are covered by the framework?

Given our response to Question 1, criticality of infrastructure entities can be assessed based on the impact of interruption to services from an economic, social, cultural and environmental perspective (not necessarily in that order). Given that we have emerged into a knowledge-based economy, the importance of access to information resources and communications is paramount. However, the inclusion of data and cloud is complex. Many services that could be deemed critical infrastructure for Australia are operated overseas, but if these services are attacked there will be implications to Australia. How the criticality of these types of services is assessed needs to be considered when determining the ontology of critical infrastructure.

Additionally, any assessment of criticality should address the strategic and operational objectives of threat actors, where such actors exist. This factor is usually not considered in critical infrastructure protection because the focus is on assessing criticality to the home nation. But cyber-attacks are better understood as campaigns where threat actors build towards an objective (rather than single incidents). Subsequently, situation awareness of threat actors and threat profiling will give an indication as to which entities would be of interest to particular threat actors. For example, one particular threat actor started with private enterprise (cyber-enabled theft of trade secrets related to a particular technology e.g. vaccinations) before undermining critical infrastructure (e.g. the health sector). See the following article in the New York Times about the race to steal the COVID-19 vaccine: [Race for Coronavirus Vaccine Pits Spy Against Spy](#)

Q6. Which entities would you expect to be owners and operators of systems of national significance?

The OCSC has worked with a number of nations in the region to understand what each country considers critical. We would expect that there would be a mix of private sector, national owned and private public partnerships that own and operate systems of national significance. The governance structure within organisations that own and operate such systems will directly affect how they see their role and responsibility in preventing and responding to cyber-attacks.

Agreeing on a shared definition for systems of national significance will assist an audit of ownership to inform related risk assessments to effectively manage associated risks and assist with aligning governance.



Government-Critical Infrastructure collaboration to support uplift

Q7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

One of the problems with TISN is that there isn't much public information about it. It should be updated or replaced by the JCSCs, with information made more widely available to ensure that government reaches all the entities it wants to reach. Restricting access to just technical cyber experts will miss out on important perspectives that may have strategic implications.

Q8. What might this new TISN model look like, and what entities should be included?

The first TISN model was developed in the 2000's. The model should be updated to reflect the current view of critical infrastructure, including as a minimum cloud and space.

Q9. 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?

A national framework for the governance of critical infrastructure protection will be instrumental in defining the specific kinds of support that critical infrastructure entities can rely upon. Given the increasing complexity of technology infrastructures and the corresponding capability required to manage and protect them from disruption and attack, a key focus must be on improving resilience and building secure systems. Further, it is critical that common frameworks and standards are defined for the assurance of both public and private critical infrastructures.

Critical infrastructure entities will require support from government to identify plausible and realistic scenarios of threat. This is particularly the case with cross-sector dependencies and with dependencies arising from constrained resources of people, process and technology. Australians must be assured that private owners and operators of critical infrastructures are delivering on their protection-related responsibilities and coordinating their effort with the relevant state/federal authorities. We therefore argue that there must be state/federal oversight on the strategic management of prevention and response to cyber-attacks. This is important for privately-held critical infrastructures as profit-seeking behaviour prioritises service availability over expensive root-cause investigations.





Initiative 1: Positive Security Obligation

The following response is a summarised answer to questions 10 – 21:

Positive security obligations can be very useful if they actually induce a change in behaviour and in systems and are not implemented as ‘tick-box’ exercises. They should provide a wide coverage of risks but point to specific action-oriented solutions. The obligations sketched out are rather high level and generic and need to be refined for particular sectors. Further, they should be extended to include processes and checks in the implementation and deployment phase of systems to ensure that organisations take responsibility of cybersecurity throughout the complete life-cycle.

A lot of the suggested obligations seem to cover best-practice type of principles and organisations in the critical infrastructure space should definitely meet most of these. Additional costs are then mainly caused by reporting and potential additional bureaucracy. If organisations do not meet large parts of the obligations, there is a need to catch up and investments should in the long run benefit the organisations by increased resilience. For some sectors it would be useful to support organisations through an independent advisory panel of experts. If obligations require substantial investments (e.g. if new interfaces need to be established to collaborate with government entities) the question of funding these needs to be part of the plan.

In general, government support is very important (Q19). It is important for the government to have a good plan and execution not only to protect critical infrastructure but also to build resilience, including a better incident reporting scheme which takes into consideration the reputational damage, further auditing concerns, incentives to encourage reporting etc. It is important that the government evaluate whether compulsory reporting or voluntary reporting will be a better fit for Australia, as many areas currently use voluntary reporting to ACSC. The revised classification of critical infrastructures can also be used to revise the reporting schemes.

Another area for essential government support is providing training and awareness. Whilst there are some areas of security training and awareness that are similar across critical infrastructure industries, there are also aspects that need to be specific to industry sectors. Training also needs to go beyond awareness. It should enable organisations to establish active (or pro-active) security.

Sharing of threat intelligence is key and needs to be pro-active and as open and accessible as possible – government can play a role in facilitating this both nationally and internationally.

Initiative 2:

Enhanced Cyber Security Obligations

Q22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

There are a number of preparatory activities that will help to remediate cyber vulnerability in Australian infrastructure organisations.

First, there is a strong need for proactive sharing of threat intelligence and vulnerabilities among critical infrastructure owners and operators. For example, the Australian finance sector has a close-knit intelligence sharing community that shares valuable information and knowledge about attacks against financial organisations across the world, and within Australia. Our top-tier banks have threat intelligence teams that draw on this intelligence to provide security management teams and incident response teams with situation awareness as well as advice on vulnerability detection and response strategy. This type of knowledge sharing would be useful to many of the critical infrastructure industries, as would knowledge sharing across the critical infrastructure landscape.

Second, the importance of research activities within the detection and remediation of cyber vulnerabilities should not be underestimated. Australia has a number of academic researchers that work in collaboration with industry from both a technical and managerial perspective with regards to cyber-security. Subsequently we recommend that there should be dedicated funding for collaborative research using Australia's Universities in partnership with industry to conduct research into new vulnerabilities, attack techniques and corresponding prevention, detection and response controls for critical networks. This should include consideration of vulnerabilities in and attacks on the integrity of the supply chain for the hardware components and software used in critical networks and systems.

Third, obligations for critical infrastructure organisations should be present for the implementation of base line security infrastructure to enable organisations to be able to identify and remediate cyber vulnerabilities. This should include the design of the cyber security infrastructure and how these systems are brought into operation. In addition to reacting to vulnerabilities, this should support organisations to prevent the occurrence of vulnerabilities.

Finally, critical infrastructure organisations should be given clear advice as to the types and level of training and awareness that employees at all levels and in all jobs should have been provided as part of the organisations obligations to protect their critical infrastructure. This would be a combination of security training (for technical employees undertaking security functions as part of their remit) as well as security awareness training (for all employees) which is targeted at their managerial level as well having a task orientation. This will, in effect over time, help to develop a culture of security within the critical infrastructure provider, which will help to reduce the likelihood of human based security threats as well as technical threats to critical infrastructure providers.



Q23. What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?

A greater sharing of information between the government and critical infrastructure would contribute to cyber resilience and result in reducing damage to society. An effective and feasible information sharing will also encourage more information sharing between entities and the government.

It is crucial for government to share with critical infrastructure entities information including recent incidents and attacks discovered and/or reported, real-time and near real-time information on newly discovered vulnerabilities and trends of cyber-attacks.

Government should also be willing to share actionable threat intelligence indicating the origin, suspected motivation and objectives of the attack, and the extent to which the attackers may have progressed in achieving their objectives. This intelligence will give defenders strategic context and situation awareness to aid and direct their response to attacks. Further, sharing validated or suspected tactics, techniques and procedures is critical for responders to shift from reactive to proactive response to cyber-attacks. Advice on defensive tactics and deployment of preventative controls can be useful especially if shared at the critical time when incident response teams are first deployed and are making sense of the incident environment and developing a course of remedial action.

It is important to explore possible mechanisms to openly share substantial information on threats. If the information is only shared with a small number of people and entities with security clearance, it will not be effective for reducing damage caused by the cyber incident or attack. An open attitude towards threat and incident information sharing will contribute to a stronger cyber security. To avoid concerns on reporting and sharing information, a better sharing platform should be established.

As argued by Chang (2012), the model used by the aviation industry in reporting 'near misses' could be a good model for government to consider improving the existing incident reporting scheme. Consideration should be given to establishing a trusted sharing platform that involves both the government and critical infrastructure entities and is not government controlled.

Q24. What could you currently contribute to a threat picture?

The OCSC would argue that understanding the cybersecurity capacity maturity of the nation across the technical and non-technical dimensions of cybersecurity is essential to inform policies, plans and practices to build resilience and protect Australia's critical assets against increasingly advanced and persistent threats.

The OCSC is the Oceania regional partner of the Global Constellation partnership that drives and delivers the Cybersecurity Capacity Maturity Model for Nations (CMM). The Global Constellation includes the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford and the Cybersecurity Capacity Centre for Southern Africa (C3SA) at the University of Cape Town. Together we conduct world leading research into national cybersecurity capacity building and resilience to understand what works, what doesn't work and why.

The CMM's holistic view of national cybersecurity includes more than 200 indicators across five dimensions: Cybersecurity Policy and Strategy; Cyber Culture and Society; Cybersecurity Education, Training and Skills; Legal and Regulatory Frameworks; Standards, Organisations, and Technologies.

Taking a multi-stakeholder approach, the CMM review process provides governments with visibility of the current situation, identifying critical gaps across all dimensions. The evidence obtained during the review process provides context informed recommendations to address gaps, lift maturity and strengthen resilience.

Since 2015 CMM reviews have been completed more than 110 times in 84 countries including the United Kingdom. Early in 2020 an independent evaluation of the CMM review process involving countries who had undertaken a CMM review was commissioned by the UK Foreign & Commonwealth Office (UK FCO). The evaluation found the following impacts from the CMM review process:

- foundational for the development of national cyber strategy and policy;
- contributes to greater collaboration within government;
- enables networking and collaboration with business and wider society;
- drives increased cybersecurity awareness locally and builds capacity;
- helps define roles and responsibilities within governments;
- enhances internal credibility of cybersecurity agenda within governments; and
- increases funding for cybersecurity capacity building.

In addition to conducting a CMM review for Australia, the OCSC could provide necessary research and threat data analysis, independent of government and industry, to provide a more detailed depiction of the threat environment and to better contribute to policy outcomes.



Would you be willing to provide that information on a voluntary basis?

As a starting point, the OCSC would be delighted to work with the Australian Government in conducting a CMM review for Australia with new benchmarking and policy reforms as a priority. The CMM's recommendations are based on evidence-based research which provides governments with foundational building blocks that strengthen National security and resilience.

Further, the OCSC is in a position to utilise its expertise to expand on any and all of the questions in this document to conduct a broader policy review across critical infrastructure and systems of national significance at the federal, state and territory levels.

What would the cost implications be?

This would depend on the scope of the project. However, working holistically top down and across with the Australian Government, a highly tailored, vigorous and detailed CMM assessment would be recommended to fit the Australian governance structure and its overall operating landscape. The estimated cost of such a review would be \$150k, more if an expanded team is required to conduct a more complex review with detailed analysis of policy across the states and territories.

Together with the Australian Government we would consider and negotiate the scope and cost of the project to ensure that the CMM review is tailored and fit for purpose.

Q25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

Critical infrastructure networks are more vulnerable to cyber threats due to their nature in providing services to the citizen and are not seen as being within a secure perimeter. Beyond agreed vulnerability scanning and penetration testing, personnel and physical security should also be tested, including social engineering techniques to gain access to facilities that house or supply services to the perimeter of critical networks. Vulnerability modelling report should be regularly prepared to study changing nature of the architecture of the infrastructure networks. Particularly modelling should include human interface and changing environment around the asset.

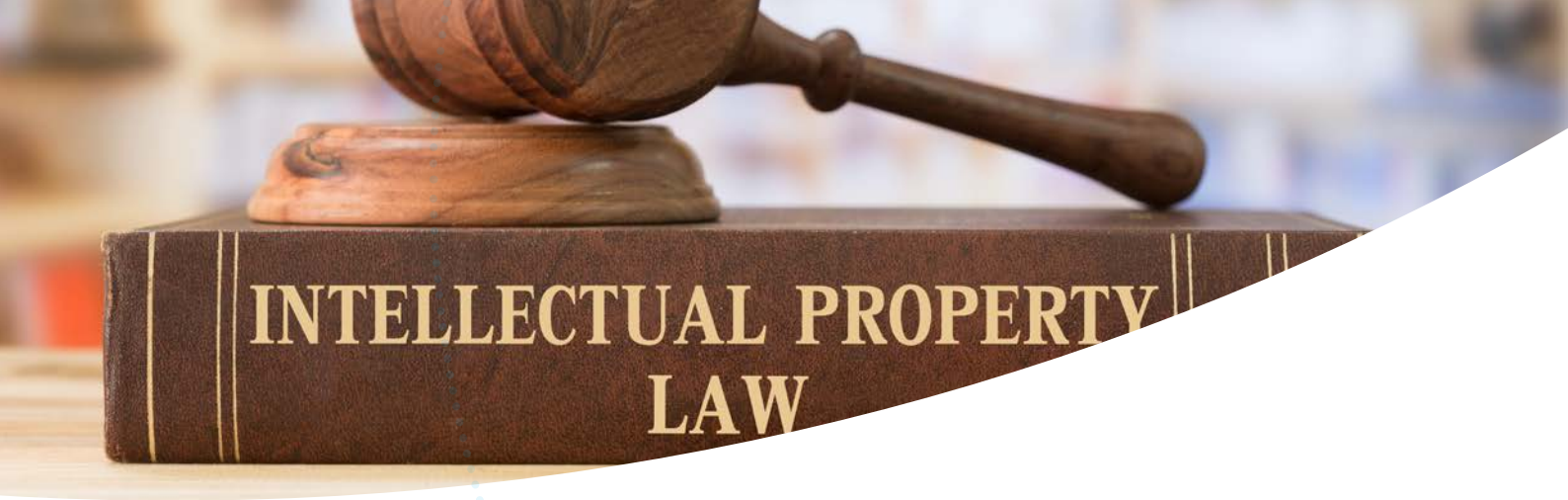
Q26. What are the barriers to owners and operators acting on information alerts from Government?

Threat intelligence and incident alerts can play an important role in directing an effective and timely response from owners and operators. Owners and operators of critical infrastructure need actionable intelligence. In this regard, the lack of context and lack of timeliness are barriers. Unfortunately, we frequently see that the lack of pre-existing trust relationships, the lack of awareness of the intelligence needs of owners and operators, and the need for secrecy and confidentiality results in intelligence being delayed and/or stripped of useful context. As a result, organisations are unable to take meaningful actions to defend themselves on the one hand, and feedback useful intelligence to authorities on the other. In the case of privately operated critical infrastructure, a key barrier is the need to restore critical infrastructure availability over expensive and lengthy root cause investigations.

Q27. What information would you like to see included in playbooks? Are there any barriers to co developing playbooks with Government?

Playbooks can play a significant role in incident response and they are strongly recommended to be developed and kept 'live' by critical infrastructure operators. It is critical that playbooks reflect the current threat landscape as well as current policies and regulations both internal and external (where relevant). A playbook should make clear how this compliance is achieved by the specified actions (both required and recommended) while at the same time ensuring that desired incident response is activated in a timely and efficient manner. Ideally, playbooks will leverage security automation and response (SOAR) platforms to the fullest extent allowing security personnel to focus on high-value and critical response activities. While playbooks tend to be heavily focussed on the technical aspects of incident response, they must also provide clear direction on how incident command, control and coordination will be managed. In a critical infrastructure context, playbooks will benefit from a sector-specific perspective that contextualises security threats and incident response strategies and actions to the sector/domain.

The benefits to industry of co-developing playbooks with government needs to be clearly articulated. Government can play a role in both facilitating and incentivising inter-/intra-sector collaborations and cooperation in terms of incident response. Trust or more specifically confidence can also be a barrier when it comes to co-developing playbooks with government. The priorities of the infrastructure operator and government if not aligned can also prove a barrier. Playbooks should reflect 'best practice' and achieve threat response with an emphasis on service continuity. It is questionable if government is able to commit the resources required to ensure that developed playbooks continue to be 'best practice' in an evolving threat landscape.



INTELLECTUAL PROPERTY LAW

The ownership of security strategy and operations should solely lie with the infrastructure operators. While government clearly has a role to play in terms of strategic policy and regulation, playbooks sit at the operational level and do not fall under this remit. Co-development of playbooks has the potential to negatively impact on the level of ownership taken by infrastructure operators in relation to their security operations in general and playbooks specifically.

Q28. What safeguards or assurances would you expect to see for information provided to Government?

Providing detailed information to government requires a combination of technical safeguards and trust. First, it needs to be clearly defined what the information will be used for and who will get access to it. Experience has shown that once data is shared the use of it is often extended beyond what was anticipated. This type of extended use of data can quickly deteriorate trust. Therefore, a first layer of protections should be applied before data is shared. It should be anonymised, or advanced cryptographic primitives can be used to enable government to learn from data without accessing the complete data set. Australian Universities have very promising research in this space and collaborate with U.S. partners on secure secret sharing and other technologies that can reduce the risk and greatly increase trust in reporting mechanisms.

Further, there can be an interesting challenge to combine reporting with compliance obligations. The risk of a fine can be very damaging to self-reporting and sharing of intelligence. Australia's legislation and behaviour around secret information and whistle blowers does not provide a good foundation for trusted sharing of critical information. Thus, safeguards protecting the source of information and strong anonymisation (without backdoors) are required for critical cases. It is important to embed 'safe harbour clauses' and ways to promote reporting. The current reporting scheme used by Aviation industry to report near misses would be a good model to consider when we design an incident reporting scheme.

Initiative 3: Cyber assistance for entities

Q29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

There are a range of responses open to a government when faced with a foreign-sourced cyber-attack ranging from diplomatic representations to count attack (see Coppel and Chang 2020). When the attack is state-backed, there is a real risk of escalation and collateral damage to other aspects of the relationships such as trade and investment. An ability and demonstrated willingness to take direct action should be an option open to government. However, it is in the national interest for any direct action to be proportionate and the most appropriate response having regards to other response options and broader interests.

The scope of direct actions and the power to take direct action should be defined in national legislation. The legislation should define who determines an extreme situation and who decides that direct action is in the national interest. For example, it should be appropriate for approval from the National Security Committee of Cabinet before a direct action is taken. This is the forum where other options and the broader implications can be considered. The legislation should also provide for the leader of the opposition to be briefed by agencies before or, in an emergency, immediate after a decision to take direct action is taken.

With regards to permissible actions, the legislation should specify what is not permissible rather than what is permissible. With technology and the nature of attacks rapidly changing, there is a real risk that the Government's response option will be unable to deal with new situation. The list of what is not permissible should reflect our values and community views. For example, actions that harm directly or indirectly humanitarian agencies might not be permissible.



References

Ahmad, A., Webb, J., Desouza, K.C., and Boorman, J. (2019). "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack," *Computers & Security*. Vol 86, pp. 402-418.

Chang, L.Y.C. (2012) *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham: Edward Elgar.

Coppel, N and Chang, L.Y.C. (2020). Cybercrime, deterrence and evading attack. *The Strategist*. Retrieved 14 September 2020 from <https://www.aspistrategist.org.au/cybercrime-deterrence-and-evading-attack/>

Desouza, K. C., Ahmad, A., Naseer, H., & Sharma, M. (2020). "Weaponizing Information Systems for Political Disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT)" *Computers & Security*. Vol 88, pp. 1-15.

Fowler, A. (Reporter), & O'Brien, K. (Presenter). (2013). *Hacked! Four Corners* [Television programme]. Sydney: NSW: ABC Television.

This submission was co-authored by the following Academic and Non-Academic Oceania Cyber Security Capacity Centre's member network:

Academic

(in alphabetical order)

Associate Professor Atif Ahmad

University of Melbourne

Dr James Boorman

Oceania Cyber Security Centre

Dr Lennon Yao-Chung Chang

Monash University

Professor Robin Doss

Deakin University

Professor Iqbal Gondal

Federation University

Dr Sean Maynard

University of Melbourne

Associate Professor Carsten Rudolph

Monash University

Professor Matthew Warren

RMIT University

Non-Academic

Ms Kate Pacalt-Shady

Head of Marketing and Communications
Oceania Cyber Security Centre



“We work at the forefront of research to strengthen cybersecurity capacity and build contextualised resilience, exploring questions of what works, what doesn’t work and why”



Door 34, Goods Shed,
Village Street, Docklands VIC 3008

Email: info@ocsc.com.au

ocsc.com.au

