UNISYS | Securing Your Tomorrow®

Ashwin Pal
Director Cyber Security | Asia Pacific
Unisys Corporation

Introduction

Unisys Australia is pleased to provide its response to the 'Protecting Critical Infrastructure and Systems of National Significance Consultation Paper 2020'.

It is encouraging to see the Federal Government drive this key initiative as the criticality of these services have been highlighted by Australians as part of the 2020 Unisys Security Index™.

The Unisys Security Index is an annual snapshot of the Australian public's security concerns, that polled 1,016 Australians in March 2020. This year it also looked at how much a two-day loss of various services would impact our work and personal lives. It found that the loss of electricity and telecommunications clearly have the biggest impact on both the work and home lives of Australians. Half of respondents (50%) said losing power at home would have the biggest impact on their personal life – more than three times higher than losing identity documents (14%) or internet coverage at home (10%) – the services with the next highest impact. Similarly, the greatest impact to work life is losing power at work (26%) and losing power at home (22%) while the loss of internet coverage at work and home had almost equal impact on work life (11% and 10% respectively) – highlighting the blurred distinction between our work and home space and lives – even pre-COVID-19.

These findings underscore the need for the security of Australia's critical infrastructure, including utilities, to be expanded and uplifted.

As the war on cyber security evolves and intensifies, policymakers face a near impossible challenge to fully understand the twists and turns, the new threat vectors, and the relative merits of technologies on offer. As the threat landscape evolves, policy makers need to embrace practical and effective precautions to reduce risk, minimise damage, and stay ahead of new threats and weapons.

Unisys recommends the Federal Government undertake three key initiatives:

1. **Educate.** The government needs to ensure the relevant critical infrastructure entities (owners & operators) have the right tools and knowledge to be secure
2. **Mandate** common standards for cybersecurity to make critical infrastructure entities more resilient. From a cybersecurity perspective, these should include the Essential Eight for IT security and the ISA99/IEC62443 standards for Operational Technology security
3. **Share.** Disseminate threat information to critical infrastructure entities and cross sector dependent entities.

Singapore successfully undertook a similar initiative in 2018 that Australia can draw best practice from. They introduced legislation (Cybersecurity Act 2018) to drive better critical infrastructure security in Singapore and published a code of practice to improve cyber security for critical infrastructure. We encourage the Australian Federal Government to take similar steps to improve the resilience of critical infrastructure entities here.

UNISYS | Securing Your Tomorrow®

Ashwin Pal
Director Cyber Security | Asia Pacific
Unisys Corporation

Responses to 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)?
    - Other sectors that should be included are:
        i. Security and emergency services (e.g. prisons, police, etc.)
        ii. Services relating to functioning of Government (e.g. electronic processing of govt. information)
        iii. Services relating to media (for secure printing, emergency broadcasts)
        iv. Transport should be clarified to include land, air and sea
        v. Energy should be clarified to include electricity, gas and petroleum and should include the entire supply chain from local generation to distribution
        vi. Each critical sectors' immediate supply chain providers.

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

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?
    - The two factors stated are the key considerations.

4. What are the common threats you routinely prepare for and those you have faced/experienced as a business?
    - Phishing attacks
    - Insider threats
    - Physical security threats
    - Attacks on Operational Technology
    - Malware
    - Nation state attacks via zero-day threats
    - Natural disasters

5. How should criticality be assessed to ensure the most important entities are covered by the framework?
    - Entities directly linked to the social and economic wellbeing of the nation, or those involved in defence and security, and their related supply chain entities should be covered by the framework.

6. Which entities would you expect to be owners and operators of systems of national significance?
    - These have to be Australian owned and operated entities to ensure they are always operating in the nation's interests without external influence or pressure.

UNISYS | Securing Your Tomorrow®

Ashwin Pal
Director Cyber Security | Asia Pacific
Unisys Corporation

Government-Critical Infrastructure collaboration to support uplift

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?
    - A revised TISN should allow better information sharing on best practices, risk and hazard identification and management, threat management and lessons learnt from experience. The TISN must provide a platform for government, academia and industry collaboration and information sharing. The TISN should be expanded to include collaboration with friendly countries to enhance resilience and cooperation with countries critical to the Australian supply chain
    - A revised and Critical Infrastructure Resilience Strategy must focus on the key principles of predict, identify, protect, detect, respond and recover underpinned by sound risk management strategies and framework. The latter will provide a model to measure and manage risk appropriately. The former (predict, identify, protect, detect, respond and recover) dictates key control areas that must be satisfied to ensure resilience.

8. What might this new TISN model look like, and what entities should be included?
    - The new TISN model should facilitate better information sharing and collaboration with the right entities. This means that the platform should allow input and sharing of relevant information (threat, risk, best practices, lessons learnt) easily into the TISN in an anonymised manner that can be shared widely. The TISN should include key supply chain entities as well as entities that provide services to critical infrastructure entities that keep them resilient in a shared responsibility model.

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?
    - Education is key. The government needs to ensure the relevant critical infrastructure entities have the right tools and knowledge to be secure
    - Mandate common standards for cyber security that can be used to make critical infrastructure entities more resilient. From a cyber security perspective, these should include the Essential Eight for IT security and the ISA99/IEC62443 standards for Operational Technology security
    - Introduce legislation to enforce the standards above. This enforcement should not be left to self-policing and should be backed by appropriate penalties for failure to comply
    - License providers of cyber security services to critical infrastructure entities to ensure basic standards are being met
    - Assist with mapping out cross sector dependencies as this may not be performed consistently, and ensure this is documented with relevant resiliency measures extended to these dependent entities in a manner similar to critical infrastructure entities. This should cover all suppliers / partners in your supply chain or ecosystem
    - Disseminate threat information to critical infrastructure entities and cross sector dependent entities

1G Homebush Bay Drive | Rhodes NSW 2138 | Australia | M: [redacted] | [redacted] | www.unisys.com

Ashwin Pal
Director Cyber Security | Asia Pacific
Unisys Corporation

- Step in to assist with major breaches or other such issues with critical infrastructure entities and cross sector dependent entities.

Initiative 1: Positive Security Obligation

Security Obligations

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

11. Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?
    - We believe that the broad security requirements do provide guidance, but are currently a little too broad to set clear expectations. Addition of expected outcomes / KPIs / measures will provide the clarity needed.

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?
    - None of the organisations that we are familiar with fully comply with these principles. These include organisations in Banking and Finance, Energy, Government (including transport and roads), etc. Depending on the type of organisation, some are better in certain areas than others. Most are weak when it comes to cyber security and supply chain security and will require cultural change and enforcement through legislation to operate in-line with these principles. In certain industries such as energy and healthcare, a period of 2-3 years and significant financial cost may be needed to meet these principles. Having said this, 'significant' is subjective and this needs to be weighed against the risk that is otherwise being taken.

13. What costs would organisations take on to meet these new obligations?
    - The costs would vary by area and include things such as investments in internal staff time, investment in external consultants, purchase of any additional equipment or tools required, cost involved in developing new processes as needed, etc.
    - The opportunity cost of not being cyber resilient must also be considered. For example, in the area of cyber risk management it is important that organisations are able to communicate cyber risk to Boards and Executives. This is one of the key reasons why businesses underinvest in cyber security and addressing this will ultimately lead to better cyber resilience for businesses. The 2019 Cyber security Standoff Australia study found that, in many instances, cyber security is still considered to be an 'IT concern' and that CEOs and CISOs are at odds with each other regarding the role of cyber security within the organisation. For example, 69% of CISOs believe that cyber security is viewed as part of the organisation's business plans and objectives; however, just 27% of CEOs agree with this statement.

Ashwin Pal
Director Cyber Security | Asia Pacific
Unisys Corporation

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?
    - The financial sector comes pretty close with the obligations imposed by APRA. The costs vary between organisations depending on size. They range from hundreds of thousands to millions of dollars in uplift and maintenance. The obligations in this case meet most principles.

Regulators

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?
    - We believe it will.

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?
    - Clear expectations backed with clear measures and timeframes, so it is obvious when non-compliance occurs
    - Clear reporting guidelines and timeframes
    - Clarity of enforcement measures and penalties.

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?
    - Using the financial sector as an example, it is APRA. Yes. The previous limitations were the ability to enforce the standards, clarity within the standards and associated penalties which were deemed too weak. These were largely addressed as a result of the Royal Commission. However, this highlights some of the potential shortcomings of regulators in other sectors. This has to be addressed to ensure another Royal Commission is not required in that sector before improvements are made.

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?
    - Funding and staffing are critical to ensure they can execute their duties adequately
    - Clarity on their role, responsibilities and powers
    - Clarity of regulations they are enforcing
    - Empowerment to enforce the requirements and penalise non-compliance.

19. How can Government better support critical infrastructure in managing their security risks?
    - Education is key. The government needs to ensure the relevant entities have the right tools and knowledge to be secure
    - Provide common standards that can be used to make critical infrastructure entities more resilient. From a cyber security perspective, these should include the Essential Eight for IT security and the ISA99/IEC62443 standards for Operational Technology security

Ashwin Pal
Director Cyber Security | Asia Pacific
Unisys Corporation

- License providers of cyber security services to critical infrastructure entities to ensure basic standards are being met
- Assist with mapping out cross sector dependencies as this may not be performed consistently and ensure this is documented with relevant resiliency measures extended to these dependent entities in a manner similar to critical infrastructure entities
- Disseminate threat information to critical infrastructure entities and cross sector dependent entities
- Support the use and innovation in automation technologies to prevent human error, automate repeatable processes/responses and free up people to do the critical thinking
- Step in to assist with major breaches or other such issues with critical infrastructure entities and cross sector dependent entities.

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?
    - The security clearance requirement should be expanded to everyone providing services to critical infrastructure providers
    - Introduce a licensing scheme for providers of services to critical infrastructure. Using cyber security as an example, two existing industry qualifications such as CISSP and CISA, etc. can be used to formally license cyber security professionals via the Australian Computer Society. This will ensure a common standard is enforced across these providers.

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

Initiative 2: Enhanced Cyber security Obligations

22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?
    - This has to be done from a risk perspective. Threats have to be identified. These then have to be matched up to identified vulnerabilities to provide probability of occurrence. This in turn has to be matched with the impact to develop an idea of the organisation's risk posture and exposure before remediation can begin.
    - Regular vulnerability assessments are key as preparatory activities. However, this has to be augmented with threat intelligence, threat hunting, Red and Blue teaming exercises augmented with attack aligned playbooks and response capabilities.

23. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?
    - Information should be shared on best practices, risk and hazard identification and management, threat management and lessons learnt from experience. This will lead

Ashwin Pal
Director Cyber Security | Asia Pacific
Unisys Corporation

to greater awareness and education in the sectors which in turn will lead to better resilience.

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?
    - Threats that we are seeing and mitigating in our line our work with our customers locally and globally. Yes. The cost will include access to a platform to share this information, personnel costs to collate and anonymise the information.

25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?
    - Regular vulnerability scans of the entire environment as it changes. Threat hunting, and Red and Blue teaming exercises.

26. What are the barriers to owners and operators acting on information alerts from Government?
    - Resources internally and motivation. The latter will need to be addressed through legislation and enforcement.

27. What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?
    - Responses to attack scenarios described by the MITRE ATT&CK framework. Playbooks for common attacks should be developed and distributed by the government. This will reduce the burden on entities and establish a common response baseline for all entities for common attacks.

28. What safeguards or assurances would you expect to see for information provided to Government?
    - The information has to be anonymised so that no personally identifiable information is communicated.
    - The information has to be protected from malicious modifications. The information will form the basis of cyber security decisions being made and incorrect information can lead to incorrect actions.

Ashwin Pal
Director Cyber Security | Asia Pacific
Unisys Corporation

Initiative 3: Cyber assistance for entities

29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?
    - Where the safety of Australians is in question, the Government must step in immediately to protect life. In these situations, a complete takeover of the entity's operations is permissible.

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?
    - This power should sit with the Federal Minister responsible. They should receive advice from the relevant regulatory body, key experts in the industry and their ministry.

31. Who should oversee the Government's use of these powers?
    - An emergency management committee should be pre-established that can oversee the use of these powers as well as the management of the emergency.

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?
    - If disruption is needed, that the use of offensive security is warranted to protect the economy, security or sovereignty of the nation. If it is a friendly nation where local law enforcement can assist **expeditiously**, then they could be called upon on to assist. In the case of a nation that does not have cordial relations with Australia, quick and decisive action directly by Australia is warranted.

33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?
    - Immunity to prosecution as long as they are operating within defined boundaries and rules of engagement. This implies that 'defined boundaries and rules of engagement' have to be established as part of this initiative and the legislation being developed. The efforts of the Singaporean government mentioned in the introduction is an example of this.

34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?
    - A pre-established committee of senior members of Government must oversee the operation. A post emergency report must be prepared and carefully analysed after the event to ensure no abuse of powers were undertaken.

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 risk to industry is directly related to the inability to quickly detect, respond and recover from a significant cyber incident. The recent Toll Holdings ransomware attacks is a clear example. Toll has to make significant investments to aggressively

Ashwin Pal
Director Cyber Security | Asia Pacific
Unisys Corporation

uplift their cyber security posture in a 12-month period. They have been forced into this position due to two breaches and years of under-investment in cyber security capability. The costs have to be borne to reduce the risk to an acceptable level. Balancing the cost of a breach against the cost of an uplift will provide the impetus to invest. Quantitative risk analysis in this case will greatly help with making this decision.

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 are adequately reflected. With the Government providing education and threat information, one would expect the private sector to be able to protect themselves better with this increased understanding. With clear guidelines AND associated measures / KPIs, the private sector should be able to uplift their resilience. Legislation and associated enforcement should provide the private sector with the motivation to comply and become more resilient.

About Unisys

Unisys has extensive experience supporting more than 240 government agencies in Australia and around the world. Unisys Australia has supported mission critical systems for both public and private sector clients in Australia for decades.

We use our understanding of Australian government security policies and controls, and our real-world experience to build and support mission critical government systems. Unisys can help the Australian Federal Government structure their environment and security controls and solutions to establish and maintain a secure environment. We welcome the opportunity to discuss our recommendations with you in more detail.

Read more about our recommendations on Cyber Resilience for the Australian Government.

Read more about how we are supporting critical infrastructure globally for clients EPM and Flowserve.