Microsoft submission to Protecting Critical Infrastructure and Systems of National Significance discussion paper

Introduction

Microsoft welcomes the opportunity to comment on the Protecting Critical Infrastructure and Systems of National Significance discussion paper. We support the Australian Government's efforts to improve the security of critical infrastructure. Microsoft's threat intelligence demonstrates that these sectors are targets of malicious cyber activity with significant potential impacts on resiliency.

The Australian Government's own threat analysis reflects the seriousness of the issue. The Australian Cyber Security Centre's (ACSC) Annual Cyber Threat Report 2019-2020[1] reported that critical infrastructure sectors, including electricity, water, health, communications and education, represented around 35 percent of reported cyber security incidents in the last year.

In its Anatomy of a Cloud Assessment and Authorisation guidance[2], the ACSC stated that effective use of cloud services offers "a range of potential cyber security benefits"[3]. Cloud services can improve security and operational resiliency for many organisations, including those operating systems of national significance or critical infrastructure. While multiple variables will impact the security and resiliency benefits that organisations ultimately derive – including the cloud user, the legacy IT environment, and the sophistication of the cloud provider – potential benefits of using cloud-based technology solutions include:

- Security as a function of greater awareness: In continuing to rely on legacy IT and related operational technologies (OT), many organisations lack awareness of their overall cyber risk exposure. The process of migrating data and services to a cloud environment can act as a forcing function for new and improved cyber risk assessments and governance efforts. Cloud migration especially enhances data governance, helping organisations increase awareness of what data they retain and how they treat it. Migrating data and services to a cloud environment can also mitigate cybersecurity risks associated with the convergence of IT-OT environments, which is taking place across many critical infrastructure sectors.

[1] https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf
[2] https://www.cyber.gov.au/acsc/view-all-content/publications/anatomy-cloud-assessment-and-authorisation#:~:text=%20Anatomy%20of%20a%20Cloud%20Assessment%20and%20Authorisation,consumers%20can%20self-authorise%20CSPs%20and%20cloud...%20More%20
[3] ibid

- Security as a core business function: Microsoft recognises that trust is a fundamental part of our business model, and we do our utmost to earn it. Cloud Service Providers more broadly, use security to differentiate themselves, hiring the best talent and investing significant resources.

- A better understanding of the threat environment: Especially for hyperscale[4] cloud providers, a large pool of clients and managed infrastructure means a wider security intelligence view, more frequent and accurate threat identification, and more proactive mitigating action. For instance, Microsoft quarantines and examines email attachments blocked by our advanced threat protection service, and if malware is found, will then use that information to proactively protect all our customers from similar threats.

- Resiliency and recoverability design principles: Hyperscale cloud providers also operate on a scale that requires them to architect their systems with resiliency at their core; they assume that nefarious users will exist, environmental disasters will happen, customer workloads may be infected with malware, and physical machines, network devices, and storage arrays may fail. Data centre replication, data mirroring, and other redundancy, failover, and recovery capabilities, used within appropriate geo-boundaries both for the platform and for customer transactions and data, are foundational aspects to how Microsoft and other hyperscale cloud providers operate our services.

- Scale as a shock absorber: Cloud resiliency also helps customers respond to emergencies and thwart distributed denial of service (DDoS) attacks more effectively than with on-premises solutions. The rapid, elastic, smart scaling of distributed cloud resources can absorb the impact of a malicious attack or an otherwise unexpected wave of access requests.

- Outsourcing of security maintenance and capabilities: Depending on the cloud service model, cloud providers may be responsible not only for data centre security but also for network controls, patching, and identity and access controls. In legacy environments, patch management and vulnerability and security configuration scanning may be irregular and even spotty, but cloud providers undertake these critical security maintenance activities as part of their service provision. Cloud providers may also manage advanced security capabilities or features, such as encryption of data while it's being processed (in addition to encryption of data while at rest and in transit).

- Security innovation: For tech providers, a focus on delivering rapidly deployed cloud solutions means that innovation is often designed for cloud environments and only later

[4] The distinction between cloud service providers and *hyperscale* cloud service providers is important to understanding the nature and sophistication of each type of entity within the broader ecosystem of organizations providing services to critical infrastructure. "In a sentence, hyperscale is a fusion of hardware and facilities with the purpose of scaling a distributed computing environment to thousands of servers" Michael Allen, Senior Vice President Solutions and Engineering at Datacenters.com: https://www.linkedin.com/pulse/what-hyperscale-how-shaping-industry-michael-allen/

translated into on-premises solutions. New features can also be rolled out to cloud customers with greater agility. Moreover, as with other domains of innovation, using cloud services enables greater use of IoT, big data, and AI, catalysing the development of new security capabilities.

While using cloud services can improve security and operational resiliency for many organisations, variability among cloud providers and cloud users impacts the extent to which these benefits can be realised, and interdependencies among sectors create new risks that warrant consideration.

Microsoft's Position on security of Critical Infrastructure and Cloud Service Providers

Ultimately, Microsoft and the Australian Government share a common goal of (1) understanding security responsibilities (those that apply separately to critical infrastructure operators and shared responsibilities between the operators and Cloud Service Providers); (2) increasing visibility into critical dependencies; and (3) exploring where greater security assurance is needed.

In our submission to the 2020 Cyber Security Strategy consultation,[5] we recommended implementing outcomes-based cybersecurity practices and security baselines for operators of Critical Infrastructure. This is largely reflected in the Positive Security Obligations (PSO) in the discussion paper.

However, in crafting and applying the Positive Security Obligations, Enhanced Cyber Security Obligations and the assistance requirements on Cloud Service Providers, the legislation should recognise the customer relationships that these organisations have with Critical Infrastructure operators who have already imposed significant compliance requirements to meet existing regulatory obligations.

Our submission makes the following recommendations:

- Separate data centres and cloud service providers in the sectoral definitions;
- Align Australian regulatory requirements with international standards and best practices based on cross-sectoral baselines;
- Map existing regulatory requirements and security obligations met by cloud service providers and harmonize those requirements to avoid duplication;
- Create protocols that ensure that the operator of the Critical Infrastructure systems, rather than the supporting cloud service provider, is the focal point for any of the proposed Enhanced Cyber Security Obligations and the Cyber Assistance requirements; and
- Create clearly identifiable thresholds and checks for the use of the Ministerial Direction powers.

[5] https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-203.pdf

Data and Cloud Sector

We understand the intention to group the data and cloud industry together given the strong linkage and that they are clearly interdependent sectors. We recommend, however, that drawing a distinction between the two would be more effective.

In many respects, the relationship between data centres and cloud services is similar to the relationship between data centres and the electricity and telecommunications sectors. Data centres are fixed, physical assets reliant on energy and telecommunications networks that connect to them. Data centres support a range of customers, including: clients that manage part of their technology infrastructure from within the data centre environment; managed service providers who might support a number of customers' technology infrastructure from within that data centre environment; and potentially cloud service providers.

As a customer of data centre providers, cloud services are computing systems and software that are logically separated from the physical hardware that run within data centre environments. The key difference between traditional information technology environments and cloud services is that the services are not necessarily tied to one physical location.

In the same way that data centres maintain redundant power supplies and telecommunications network connections; hyperscale cloud providers maintain and distribute services across multiple data centre sites to ensure continuity of service delivery.

Even when services maintain data at rest within one nation's borders, such as Microsoft's services hosted in Australia, these services may be hosted across multiple data centre sites with different operators to ensure redundancy and resiliency of the service. In turn, these services will be maintained through a connected set of global processes and operations.

Similarly, the risk profile of data centres and cloud services are related but distinct. The threats to data centres are often connected to physical controls and personnel access or from disruptions to energy supplies or telecommunications network connectivity; while risks to cloud service providers more often relate to potential software vulnerabilities and virtual access to data.

Creating separate designations for data centres and cloud service providers will enable governments to better focus on each sector's unique threats and interdependencies and the differing relationship that both have with other Critical Infrastructure operators as suppliers and customers.

Separate designations would also enable the government to scope a cloud services designation in a way that focuses risk management attention on services that are used for more critical functions among other CI providers. Cloud services are a broad category that risks diverting attention to services on which there are few dependencies and applying requirements in a way that inhibits new providers and less critical services from market access. Alternatively, a risk-based approach to

scoping a cloud services designation requires greater understanding of CI interdependencies and results in a focused application of efforts to advance security and resiliency.

Alignment with Global Best Practice

Cloud services are different than other 'industry vertical' sectors. Digital technologies cut across the entire economy, serving a broad swathe of industry verticals, and often also serve a global customer base. Microsoft therefore appreciates that evaluating the criticality of cloud services is a necessary part of a broader effort to understand and manage risk associated with increasing interdependencies. Across sectors and organisations, complex, overlapping supply chains and common leveraging of digital technologies and services contribute to such interdependencies. In addition, future visions for smart cities and platforms like smart highways reveal the potential for further sectoral integration.

We urge that the regulatory effort recognise and embrace these interdependencies, which (1) recognise separate and shared responsibilities between operators and cloud service providers; (2) require an approach that is interoperable across sectors; (3) should align with international best practice and standards for providers and operators that work across multiple jurisdictions; and (4) recognise that the threats and the technologies in the cloud will evolve over time; assuring that operators and service providers can evolve accordingly will be paramount.

First, the unique nature of cloud service providers' relationships with customers means that effective regulation requires an understanding of separate (those directly on the critical infrastructure operator) and shared (applying to both the operator and the cloud service provider) responsibilities for cloud security. In this respect, imposing new security controls and reporting obligations just on the cloud service provider may have the unintended consequence of undermining security arrangements that already exist and are operational.[6]

Second, increasing and forthcoming interdependencies among critical sectors demonstrate the need for cross-sector interoperability of security requirements. Even today, supply chain integration and common leveraging of services mean that cloud providers and other organisations must meet the security requirements of multiple sectors. Moreover, beyond regulatory and compliance impacts, interoperable approaches facilitate use of a common language, increasing understanding of cyber risk management practices across supply chains and helping to illuminate where gaps may exist.

Cross-sector baselines for cyber risk management enable interoperability while also allowing for sectoral variation that's grounded in demonstrated need. Security baselines are a foundational set of policies, outcomes, activities, practices, and/or controls that help to manage a range of

[6] We discuss this recommendation in greater depth in a subsequent section of our submission.

cyber risks that are applicable across most environments.[7] Many risks faced by critical infrastructure and systems of national significance are similar, so cross-sector "baselines" address a significant majority of cyber risks applicable across organisations. To address risk scenarios that are unique to different critical infrastructure sectors or organisations, security baselines may be augmented with a narrow set of sector-specific requirements.

Finally, cloud services – and hyperscale cloud providers in particular – often operate global services and therefore benefit from compliance with global security standards and international best practices. Likewise, governments benefit their own operations and those of domestic companies by using international standards, gaining efficiencies in assurance efforts, enabling more streamlined international cooperation, and supporting integration with international supply chains and markets. New security obligations in Australia relating to critical infrastructure should leverage international standards, thereby contributing to more harmonised security obligations worldwide.

Existing best practices and international standards provide useful frameworks for cross-sector baselines, and they support not only cross-sector but also cross-region interoperability. ISO/IEC 27101 articulates cybersecurity framework development guidelines that are applicable across sectors.[8] It also incorporates ISO/IEC 27103, which provides guidance on how to use existing ISO and IEC standards to implement risk management activities required by a cybersecurity framework.[9] As a starting point, ISO/IEC 27103 leverages the *Framework for Improving Critical Infrastructure Cybersecurity*, commonly referred to as the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[10] which numerous global critical infrastructure organizations acknowledge the benefits of using.[11] Financial services, IT, and telecommunications providers have described how a common security baseline across ISO/IEC 27103, the NIST Cybersecurity Framework, and sector-specific frameworks enables consistency and interoperability while also addressing unique concerns of their regulators.[12]

Mapping existing requirements

Just as the use of existing best practices for cross-sector security baselines can help to enable interoperability and achieve efficiencies while maintaining a high bar for security and resiliency, use of existing or in-development cloud security certifications and international standards-based compliance frameworks can yield tremendous benefits.

---

[7] http://download.microsoft.com/download/4/6/0/46041159-48FB-464A-B92A-80A2E30B78F3/MS-riskmanagement-securitybaselines-WEB.pdf (describing how security baselines may cover policy goals – e.g., protecting against cyber threats, more specific desired outcomes – e.g., know your organizational risks, security activities or practices – e.g., conduct a risk assessment, and security controls at 6)

[8] https://www.iso.org/standard/72435.html

[9] https://www.iso.org/standard/72435.html

[10] https://www.nist.gov/cyberframework

[11] https://www.nist.gov/industry-impacts/cybersecurity-framework (highlighting use by Boeing, J.P. Morgan Chase, Nippon Telegraph and Telephone Corporation, and the Bank of England among others); *see also* https://www.nist.gov/cyberframework/perspectives

[12] https://www.crx2.org/s/CR2-White-Paper_Seamless-Security.pdf

Many cloud providers have already invested significantly in certification programs, which often require security and resiliency practices that are consistent with what's required for the storage and processing of classified government information – an appropriately high bar commensurate with the requirements that are applied to other critical infrastructure and essential services organisations as well.

Given the broad use of Microsoft cloud services across a range of regulated industries, Microsoft has demonstrated compliance with a number of global and local standards and regulatory requirements. At this point in time, there are more than 90 separate certifications or compliance reporting mechanisms that Microsoft maintains across the globe[13]. Because cloud services operate from a single set of security controls, additional controls to meet these global compliance requirements become a core part of how the service operates.

In Australia, this includes maintaining valid Information security Registered Assessor Program (IRAP) assessments to support Australian Government agencies' compliance with the Information Security Manual (ISM); and a series of regularly revised guidance that assists financial institutions' compliance with the Australian Prudential Regulation Authority's (APRA) Prudential Standard CPS 231 Outsourcing[14] when outsourcing a material business activity and ongoing compliance with Prudential Standard CPS 234 Information Security[15]. Microsoft has also provided detailed guidance for financial services with responses to each issue raised in the APRA Information Paper Outsourcing involving cloud computing services[16].

Both the ISM and the APRA guidelines provide good risk-based frameworks that enable cloud service providers and regulated entities to engage in risk-based approaches to the adoption and ongoing management of cloud services in a broader framework of security controls that also apply to on-premise technology.

This is critical, because while the growth in the use of cloud services demonstrates the importance of having visibility and assurance in the cloud context, many critical infrastructure operators also continue to leverage on-premises or hybrid solutions. A holistic understanding of risk exposure and risk management is key to ensuring security and resiliency both within and across critical sectors.

We recommend that before the Positive Security Obligations and Enhanced Cyber Security Obligations are finalised, the Government undertakes a detailed mapping exercise of existing sector-specific requirements to ensure that new obligations don't create duplicative reporting and compliance requirements. To the greatest extent applicable, governments should enable cloud service providers to leverage these domestic and global certifications to provide assurance that

[13] https://azure.microsoft.com/en-us/resources/microsoft-azure-compliance-offerings/
[14] https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf
[15] https://www.legislation.gov.au/Details/F2018L01745
[16] https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf

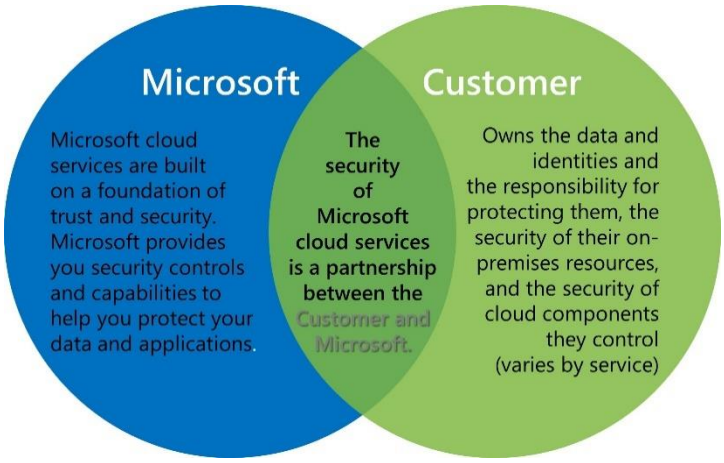
they meet any new security and resiliency requirements, limiting resource-intensive redundancies for both cloud providers and independent assessors.

Protocols for engagement with cloud service providers

The use of cloud services is governed by what is referred to as a shared responsibility matrix. Depending on the nature of the service, the cloud service provider is responsible for certain elements, such as the operation and security of the underlying cloud service, while the customer is responsible for configuring the service, managing its data and the interoperation of the cloud service with other IT services (either alternative providers or on-premise).

This effectively creates a partnership on security between the cloud service provider and the customer (see Figure 1).

Figure 1: Partnership on Security



This relationship between provider and customer needs to be recognised in the more active security obligations envisaged under the new Critical Infrastructure protection arrangements – particularly the Cyber Assistance for Entities.

In the case of the detection of an imminent threat or in an emergency scenario that is targeting a critical infrastructure entity who is the customer of a cloud service provider, it is only that entity that can determine what information is the target of such a threat or the criticality of the targeted systems to the operation of that critical infrastructure. The cloud service provider's visibility may only extend to the services that that entity is accessing and if the threat vector involves the cloud services.

In that scenario, it should be the choice of the critical infrastructure operator as to whether to involve the cloud service provider in any cyber situational awareness or cyber assistance activity that follow either from incident reporting or from threat intelligence gathered by Australia's security agencies such as ASD/ACSC.

While we know that the Australian Government plays a critical role in keeping the public safe and sometimes requires access to data or forensic evidence to do so, we also believe that our customers deserve predictability about what happens with their data and must retain ownership of their data.[17]

To enable governments' cyber defensive strategies and response planning while also protecting the rights of cloud customers in their jurisdictions, we encourage governments to codify approaches to access request scenarios that: a) put the onus on directly impacted CI operators to engage with their cloud provider and with ASD/ACSC; and b) require that any direct requests to cloud providers be narrowly tailored, require mandatory notice to and approval by the CI operator, and follow applicable legal processes that allow for judicial review.

Where governments determine that interdependencies might necessitate quick action across multiple sectors or entities, pre-established arrangements for reporting could fast track engagement and response.

Part of this protocol of engagement is having a clearly defined requirement for incident reporting. To assist with this consideration, Microsoft has defined a set of principles for the disclosure of security incident information:

- Define outcomes and partner with industry: Keeping the Enhanced Cyber Security Obligations broad is likely to result in the reporting of incident information that is not actionable or relevant to security and economic resiliency objectives that are core to the protection of critical infrastructure and systems of national significance.
- Clearly define the responsible entity for reporting: Cyber Incident reporting requirements should fall on the impacted critical infrastructure operate rather than its service provider. This align to the mandatory data breach notification requirements under the *Privacy Act 1988* where it is the APP entity that collected the PII who must determine whether serious harm has been caused and then notify the impacted individuals. In that scenario, cloud service providers cannot see what data has been impacted even if they detect the intrusion and notify the entity. Similarly, the reporting obligation under the Enhanced Cyber Security Obligations should sit with the impacted Critical Infrastructure entity as they will be best place to assess the severity of the intrusion even if the cloud service provider detects it.
- Avoid duplicative requirements and mandatory timelines: The roles and responsibilities between the sector regulators, the CIC and ACSC should be clearly defined so as not to require multiple disclosures to multiple regulatory agencies in the event of one security incident. In addition, timelines for reporting incidents should be mapped to goals and the severity of the incident. Artificially short timelines may elicit incomplete or inaccurate data

[17] https://blogs.microsoft.com/datalaw/our-practices/

and undermine shared priorities, such as efforts to minimise the impacts of and resolve any issues associated with an incident.

- Encourage voluntary information sharing: Voluntary sharing schemes remain one of the most effective cybersecurity risk management tools. As flagged in the Situational Awareness proposals – trust between government and the private sector can be fostered by sharing actionable information. This will also necessitate leadership from the Government to share information with all relevant parties in order to ensure that it can be actioned appropriately, given the threat.
- Develop a reporting structure and ensure information is used: Technical capabilities should be put in place between relevant sector regulators, CIC and the ACSC to adequately transmit, manage, store, and safeguard incident-related data.

Thresholds for the use of Ministerial Direction and Response Actions

Under the Cyber Assistance for Entities initiative, the discussion paper references the ability for Government to take action and direct entities to work with its agencies in *"limited circumstances where Government identifies an immediate and serious cyber threat to Australia's economy, security or sovereignty (including threat to life)."*[18]

While we acknowledge that there may be emergency scenarios where the Government may consider the need for direct action with critical infrastructure operators, we believe such actions must only occur as a last resort, under a framework that incorporates robust checks and balances, as well as the Commonwealth Ombudsman acting on behalf of the private sector that reflects the interests and risks of undertaking such an action.

The use of such powers should be subject to a significant threshold, time limited and require independent authorisation. In the rare instances where ministerial direction is warranted, we recommend that it be narrowed to apply to circumstances in which gaps in abilities to defend and repel cyberthreat activity have been demonstrated during joint preparedness exercises among the government and private sector.

Microsoft, as an example of a hyperscale cloud provider, spends over $1 billion per annum on cybersecurity and has a demonstrated ability to defend itself against significant and repeated cyber threats. We also continue to work cooperatively with cybersecurity agencies like the ACSC to share threat intelligence and to respond to cyber incidents. We recommend that the proposed assistance framework recognise these demonstrable capabilities and existing collaboration.

Such a framework should also carefully consider impacts from direct action on services that are used by many thousands of Australian businesses.

[18] Protecting Critical Infrastructure and Systems of National Significance Consultation Paper, August 2020, Department of Home Affairs.

Given the complexities and interdependencies, in addition to conducting joint preparedness exercises, we recommend that the Government form a working group of cloud service providers to define these thresholds and explore the establishment of pre-defined collaborative arrangements.

Building trust and confidence in collaborative mechanisms between industry and security agencies will ultimately lead to a more sustainable and cooperative relationship that will serve Australia well should an emergency scenario arise.

We also recommend that such direct action should be limited to protective threat response activities and not be authorised to conduct, or compel private entities to engage in, cyber-offensive activities from within the networks of Critical Infrastructure operators or their service providers.