Microsoft Submission to the 2020 Cyber Security Strategy Consultation

Microsoft is pleased to respond to the consultation and discussion paper in the development of the Australian Government's Cyber Security Strategy 2020. We commend Australia's efforts to both regularly update its strategy and take a holistic approach, posing questions on topics ranging from the threat environment to protection of critical systems to awareness raising and tools to empower consumers.

As the consultation and discussion paper highlights, cyber threat activity continues to increase in both frequency and sophistication. In addition to fighting global malware and managing security response through our Digital Crimes Unit and Cyber Defence Operations Center, through our Threat Intelligence Center, Microsoft tracks escalating activity by advanced criminal networks as well as dozens of nation-state actors[1]. In July, we acknowledged that, in the last year, we had notified nearly 10,000 customers that they had been targeted or compromised by nation-state attacks.[2]

Moreover, escalating attacks are not just about computers attacking computers – these attacks threaten and often harm the lives and livelihoods of real people, including their ability to access basic services like heath, banking and electricity. In May 2017, in just a few hours, the WannaCry attack impacted more than 300,000 computers in 150 countries, including systems that supported the National Health Service in Great Britain. Six weeks later, NotPetya disabled an estimated 10 percent of all computers in Ukraine, crippling businesses, transit systems and banks, disrupted the systems of multinational corporations in other regions, and suspended operations of one of the world's leading shipping companies.

Managing escalating threats and advancing cybersecurity while continuing to support innovation and growth requires an approach that is not only multinational, but also multistakeholder in nature, harnessing industry input. This is because many critical elements of cyberspace, unlike the traditional planes of warfare like land, sea and air, are typically privately owned or operated. Cyberspace consists of concrete elements in the real world, such as datacentres, undersea cables, laptops and mobile devices. These are also mostly designed, manufactured, distributed, and managed by private companies.

[1] https://www.technologyreview.com/s/614646/inside-the-microsoft-team-tracking-the-worlds-most-dangerous-hackers/

[2] https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/

The technology sector has the first and highest responsibility to protect this infrastructure and the people who rely upon it. To this point, every day we have 3,500 Microsoft security professionals protecting our customers, and we leverage advanced AI to analyse 6.5 trillion global signals and detect and respond to threats. However, cybersecurity is ultimately an issue that requires that governments, companies and civil society to come together.

Critical infrastructure protection similarly requires cooperation between the public and private sectors because, while the resilience of these sectors is a national security priority, the critical infrastructure itself is most often owned and operated by private industry and dependent on the technologies that are developed and maintained by private companies.

Developing effective policies to respond to cybersecurity challenges requires more than a whole-of-government response; it involves a whole-of-nation effort, with government agencies like the Department of Home Affairs and the Australian Cyber Security Centre; experts from across all sectors of the economy and from civil society collaborating to create approaches that simultaneously improve security and enable innovation.

Principles

As the Australian Government moves to develop its 2020 Cyber Security Strategy, it can be useful to establish a set of principles that can act as a guidepost for the initiatives within it. In our Cybersecurity Policy Framework[3], Microsoft recommends considering six foundational principles, which provide a useful set of ideas and concepts for the development of the Australian Government's updated national strategy:

1. **Risk-based and proportionate.** Regulations and policy should be based on a thorough understanding of the threats, vulnerabilities, and potential consequences facing Australia. We also need to consider the fact that the definition of "risk" itself is changing. In the past, "risk" may have meant doing something new or adopting a disruptive new technology. Today, "risk" can result from standing still, because organisations and even countries that stand still will not only lose competitiveness but also miss out on new capabilities designed to be responsive to emerging threats, including new offensive tactics. Regulations can manage this by introducing a risk-based framework that helps organisations prioritise and focus resources on their most important assets or services, continuously improve security measures rather than be locked into a static approach, and innovate and adopt new technologies without exposing Australia to unnecessary cybersecurity risks.

[3] Microsoft Cybersecurity Policy Framework: https://www.microsoft.com/en-us/cybersecurity/content-hub/Cybersecurity-Policy-Framework

2. **Outcome-focused.** It is essential that policies and future regulation focus on delivering the desired end state, rather than prescribing the means to achieve it, and then measure progress towards that end state. In the rapidly changing world of cybersecurity, prescriptive approaches will quickly become out-of-date or leave Australia out-of-step with international best practices. Alternatively, outcome-focused approaches help organisations not only focus on security but also have greater agility as the technology and threat environments continue to evolve.

3. **Prioritised**. Not all threats are equal. National cybersecurity strategies should adopt a graduated approach to criticality, prioritising risks with greater potential impacts on national resiliency, such as critical infrastructure risks or government use of technology.

4. **Practicable and realistic**. Cybersecurity policies are of little value if they impose undue burdens on the organisations that must comply with them or on the authorities tasked with enforcing compliance. Engagement with industry and the relevant authorities is a necessary first step to ensuring that policies are practicable and realistic. As it is focused on facilitating such engagement, we commend the consultation on the Strategy that the Australian Government is undertaking.

5. **Respectful of privacy, human rights and rule of law**. Advancing security cannot come at a cost of sacrificing privacy, human rights and rule of law. For example, broad rights for government and law enforcement to access data without following appropriate processes can cut across these fundamental principles. This in turn can damage the country's reputation for rule of law and ultimately disincentivise organisations from storing their data within the country. Instead, a balanced approach is needed that is respectful of these fundamental principles.

6. **Globally-relevant.** The threats to cyberspace do not stop at national borders. It is therefore essential that governments adopt approaches for tackling cybercrime and encouraging cybersecurity that acknowledge that reality. National approaches should therefore integrate international standards to the maximum extent possible, keeping the goal of interoperability in mind wherever possible.

Governance Functions

Across a range of issues, multifaceted interaction among internal government and regulatory stakeholders, external stakeholders from the private sector, and international entities is critical. Microsoft recommends that five government functions[4] are prioritised; in

[4]ibid

Australia, these functions are largely managed across ACSC, the Department of Home Affairs and the Department of Foreign Affairs and Trade.

1. **Policy and planning function:** lead the nation's development, coordination, alignment, and integration of cybersecurity policies, strategies and plans.
2. **Outreach and partnership function:** lead and manage relationships and interfaces across the government and with other nations, institutions, and the private sector.
3. **Communications function:** coordinate regulatory and non-regulatory communication, including messages, documents and publications, and statements, to all stakeholders on behalf of relevant government authorities; manage communication during a crisis or emergency; act as a point of contact for media, organisations and the general public seeking information about programs, policies, procedures, statistics, and services. A greater focus and investment in the Communications function is worth considering as a part of the 2020 strategy.
4. **Operations function:** ensure effective coordination and deployment of resources in response to cyber threats and incidents.
5. **Regulatory function:** oversee compliance with cybersecurity regulations, including by developing guidance to help organisations understand the relevant requirements, interacting with regulators who will enforce compliance, establishing an incident reporting framework, and collaborating with other units to update regulatory obligations.

If the desire is to maintain the current structure, the Government should consider whether the existing governance arrangements are ensuring that cyber functions performed by the Australian Government are collaborative and coordinated. One possible improvement could be to have a single Coordinating Minister and/or a Coordinating Executive with oversight across all cyber functions within the existing Machinery of Government arrangements.

Critical Infrastructure

Today, cyberattacks from increasingly sophisticated actors threaten organisations across every sector, and whether a large ASX 100 company or a local bakery, organisations of all sizes need to take steps to limit the dangers posed by these threats. This is the core of cybersecurity risk management—understanding potential threats and actively working to mitigate them. But while organisations large and small should protect themselves against such threats, the owners and operators of critical infrastructure have a unique additional obligation to understand risks and improve their cyber resilience in the interests of the communities, and even whole societies, that rely on their industries.

The Australian and state and territory governments share the following definition of critical infrastructure: *'those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security'*.[5]

Based on our global experiences, further steps that we would recommend for organisations that meet those criteria include:

- **Empower the Critical Infrastructure Centre (CIC) and ACSC to implement critical infrastructure cyber protection policies:** Within the existing framework for protecting critical infrastructure, the Strategy should include the following focus areas: i) coordinating the adoption of outcome-based cybersecurity practices; ii) establishing an incentives-based cybersecurity program to encourage the implementation of outcome-based practices; iii) developing procedures to inform owners and operators of cyber-threats, vulnerabilities and consequences; and iv) providing technical guidance and support.
- **Introduce minimum security baselines for critical infrastructure:** The ACSC and CIC should establish minimum security baselines for critical infrastructure. In our publication entitled Risk Management for Cybersecurity: Security Baselines,[6] Microsoft recommends the use of security baselines for improving cybersecurity across a range of critical infrastructure environments. Such baselines could take the form of voluntary guidance, coupled with incentives, or be implemented through a mandatory regulatory requirement, where an elevated need for assurance arises from the risk environment. The measures that apply should be proportionate to the criticality of the infrastructure and based on international best practice standards, such as those set out under the National Institute of Standards and Technology (NIST) Cybersecurity Framework or ISO/IEC 27013, "Cybersecurity and ISO and IEC Standards," which provides guidance on how to leverage existing international standards in a cybersecurity framework.[7]
- **Manage supply chain risks:** Arrangements put in place for critical infrastructure operators, such as security baselines, should extend to their suppliers. This can significantly reduce risk across critical infrastructure supply chains but has the added

[5] https://cicentre.gov.au/infrastructure
[6] Risk Management for Cybersecurity: Security Baselines: http://download.microsoft.com/download/4/6/0/46041159-48FB-464A-B92A-80A2E30B78F3/MS-riskmanagement-securitybaselines-WEB.pdf
[7] https://www.iso.org/standard/72437.html

benefit of driving greater cybersecurity awareness and hygiene across the Australian economy.

- **Encourage information sharing:** Sharing threat-based information such as vulnerabilities, hacking trend data, new threat identification, or even unexplained anomalies impacting a product or service can enable the IT sector and government to better protect critical systems and respond to emerging issues. Building on the longstanding Trusted Information Sharing Network (TISN) arrangements - Microsoft believes that a sustainable information sharing program needs to be event-driven and to focus on several key areas that should be precisely defined: the actors involved, the type of information exchanged, whether sharing is voluntary or required, the methods and mechanisms for transmitting information, and the grouping of actors in a program.

Maintaining trust in an Internet of Things

The Internet of Things (IoT) is a key element of global digital transformation. While there is no universally agreed definition of IoT, it has been described at a high level as a decentralised network of devices, applications, and services that can sense, process, communicate, and take action based on data inputs, including control of elements of the physical world.

The benefits of IoT are significant. Many businesses are already streamlining their operations, managing resources more effectively and moving to more predictable maintenance schedules as connected devices provide actionable data. Like any other IT network – this growing network of devices needs to secure and maintaining trust in these systems is critical if the Australian economy is to continue to benefit from their deployment.

In a recent publication, *Cybersecurity policy for the Internet of Things*[8], Microsoft made several recommendations to help governments develop policies that advance IoT security.

These recommendations include:

- **Raising awareness of best security practices and guidelines:** Not every business has the knowledge and expertise to make smart decisions about security when developing and deploying IoT devices and services. Governments can enable better security outcomes by promoting best practices that range from security-by-design principles to sector-specific product development and risk assessment guides.
- **Developing enhanced guidance for safety critical sectors:** Greater investments in cybersecurity and system resilience apply in particular to devices that support human

[8] Cybersecurity policy for the Internet of Things: https://www.microsoft.com/en-us/cybersecurity/content-hub/Cybersecurity-policy-for-IoT

life, critical infrastructure, transportation, and other essential functions, whose inability to function and lack of resilience could have dire consequences.

- **Investing in IoT security training, education, and raise public awareness:** Government investments in workforce development and awareness-raising campaigns can help increase the scale and impact of industry-led efforts.

The Australian Government may also wish to explore the introduction of a **certification regime** related to devices. The primary goal of a certification program should be to improve security by providing more information to consumers and incentivising the broader IoT marketplace.

As the Discussion Paper references, the European Union's (EU) Network and Information Systems Directive has established a range of initiatives to drive a greater focus on cybersecurity across EU Member States.

In June 2019, the EU Cybersecurity Act came into force, creating the EU-wide legal framework, including the establishment of an EU framework for cybersecurity certification[9]. This allows for the certification of products, processes and services that will be valid throughout the EU.

This framework creates a flexible regime that leverages existing international standards; allows for self-assessment and third-party evaluation; and different levels of assurance (basic, substantial and high) that will depend on the intended use of the product or service. The governance structures will also enable a broad group of stakeholders, including industry representatives to be involved in the framework, including the development of certifications and standardisation processes.

Microsoft's position is that IoT certification programs should be informed by an open and transparent multi-stakeholder consultative process, aligned with international standardisation efforts and be flexible in implementation to accommodate the wide variety of IoT deployments possible. IoT security technologies, standards and the ecosystem are improving rapidly. The Australian Government should consider aligning any proposed certification regime with evolving IoT certification best practices elsewhere in the world.

There is already precedent in medical device regulation for this type of alignment of Australian certification processes with the equivalent processes used in other nations. The Therapeutic Goods Administration has accepted certification from the European notified bodies designated by the medical device regulators of European member states, the United States Food and Drug Administration and other similar authorities as evidence of compliance with the conformity assessment procedures in Australia.[10]

[9] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
[10] https://www.tga.gov.au/comparable-overseas-regulators-medical-device-applications

Skills

Every employee, from executive leadership to the rank and file, now has cybersecurity responsibilities. Initiatives aimed at increasing cybersecurity awareness and encouraging the public to protect themselves online have therefore proliferated. However, having professional staff dedicated to securing technology is also essential.

Large businesses and governments have tasked chief information security officers (CISOs) with building cybersecurity teams to keep sensitive data out of the wrong hands. Yet all of them face the same hiring challenge – there are not enough trained specialists to fill this critical need.

In AustCyber's second annual update to its Cyber Security Sector Competitiveness Plan released in 2018, they estimated that the Australian information security sector is 2300 workers short of demand, and Australia is expected to need up to 17,600 additional cyber security workers by 2026.

This problem can perhaps not be solved immediately; however, building on the initiatives of the 2016 Strategy, the Government can take several steps to address the cybersecurity skills gap in the near-, mid-, and long-term:

- **Utilise new technologies.** In the short term, it is important to investigate available technologies that can reduce the exposure to cybersecurity threats. For example, leveraging cloud services enable a smaller number of information technology (IT) professionals to centrally manage certain aspects of security, e.g. patch management, device management or access rights. Leveraging the cloud also brings with it the herd immunity that comes from tens of millions of users and cloud service providers like Microsoft that are monitoring and responding to global threats in real-time.
- **Embed cyber training into other areas of study.** Building on the work of initiatives of the Cyber Security Cross Sector project under the Australian Industry Skills Council and the outreach and projects funded by AustCyber – the Strategy should explore growing the baseline of cyber awareness across the education system at all levels. Growing the availability of short courses and micro-credentials should be a priority. The strategy should also consider increased support and incentives for executive training, leveraging initiatives like the partnership between the Australian Information Security Association (AISA) and Australian Institute of Company Directors aimed at developing directors' understanding of their roles and responsibilities in governing data security.
- **Encourage the establishment of cybersecurity apprenticeships or traineeships**. Given the forecast shortage in University graduates – leveraging the VET sector is critical to

ensuring the broadening of the cybersecurity skills base. The Certificate IV and Advanced Diploma in Cyber Security that is now available through nearly every State and Territory TAFE system is a great example of Public-Private Partnership to address the growing skills shortage. The Government should leverage this base and explore incentivising traineeship and apprenticeship programs that combine qualifications and industry certifications with on-the-job learning and development to more quickly grow the pool of cyber-capable IT professionals. The Microsoft Traineeship program[11] is an example of this model that is already operating for broader IT skillsets.

- **Prepare for automation of cybersecurity skills.** In the near future, many cybersecurity functions will be automated. Indeed, organisations are already using technology to increase speed of response, to understand trends hidden to the naked eye, and to offset the cybersecurity skills shortage. As a result, cybersecurity professionals will have to be trained to add value by dealing with more advanced threats and by utilising emerging techniques like AI and machine learning.

Microsoft Resources:

To support government policymakers and cybersecurity professionals, Microsoft regularly publishes a range of content that may be useful for the 2020 Cyber Security Strategy development team.

Some useful sites include

- Microsoft Cyber Security Content Hub: https://www.microsoft.com/en-us/cybersecurity/content-hub
- Microsoft Cyber Security Blog Hub: https://www.microsoft.com/en-us/cybersecurity/blog-hub
- Microsoft On the Issues: https://blogs.microsoft.com/on-the-issues/
- Microsoft Security Blog: https://www.microsoft.com/security/blog/
- Microsoft Security Resources (Webinars, Whitepapers and Training): https://www.microsoft.com/en-us/security/resources

[11] https://www.microsoft.com/en-au/microsoft-traineeship-program