Microsoft

Submission to the Government's 2023-2030 Australian Cyber Security Strategy Consultation

15 April 2023

Contents

Introduction

We welcome the opportunity to respond to the Government's consultation for the 2023-2030 Cyber Security Strategy. The initiative is a unique opportunity to establish the clear foundations that will enable greater use of data and digital technology in an era of rapid technological change and increasing global threats.

In 2023, Microsoft is celebrating being part of Australia's tech ecosystem for 40 years. With over 2,000 employees based in every state and territory in Australia, and over 9,000 partners who are predominantly small businesses employing 200,000 Australians, we have a deep history of investing locally, including in data centres that power Governments, businesses, schools and universities, and the not-for-profit sector in Australia.

Microsoft invests more than USD $4 billion in security annually and has over 8500 engineers available for our Cyber Defence Operations Centre (CDOC). We invest in highly skilled and dedicated cyber teams such as the Microsoft Threat Intelligence Centre (MSTIC), the Microsoft Digital Crimes Unit (DCU), the Digital Security Unit (DSU) and the Digital Threat Analysis Centre (DTAC).

Priority recommendation

Microsoft's priority recommendation is that the Australian Government's 2023-2030 Cyber Security Strategy promotes a flexible risk-based regulatory environment that encourages the deployment of globally competitive advanced technologies and enables the Government to build private/public partnerships with major technology, telecommunication and other critical service providers.

The scale and sophistication of cyber-attacks is rapidly increasing, and the global nature of the threat means access for the Australian Government and organisation, to the most advanced protection capabilities is the most effective way to ensure that critical infrastructure and government systems are resilient, and Australia has a secure economy.

Lessons from the conflict in Ukraine

The importance of proven cyber defences to protect key datasets has been clearly demonstrated by the Russian invasion of Ukraine. The internet's global pathways mean that cyber activities erase much of the longstanding protection provided by borders, walls, and oceans. And the internet itself, unlike land, sea, and the air, is a human creation that relies on a combination of public and private- sector ownership, operation, and protection.

Microsoft security teams have worked closely with Ukrainian government officials and cybersecurity staff at government organisations and private enterprises to identify and remediate threat activity against Ukrainian networks. When the Microsoft Threat Intelligence Center discovered wiper malware in more than a dozen networks in Ukraine, we alerted the Ukrainian government and published our findings.

Following that incident, we established a secure line of communication with key cyber officials in Ukraine to be sure that we could act rapidly with trusted partners to help Ukrainian government agencies, enterprises and organisations defend against attacks. This has included 24/7 sharing of threat intelligence and deployment of technical countermeasures to defeat the observed malware.

We believe there are a number of conclusions from the Russian invasion of Ukraine that are critical when considering cyber security in Australia.

I. First, defence against a military invasion now requires for most countries the ability to disburse and distribute digital operations and data assets across borders and into other countries. Russia not surprisingly targeted Ukraine's governmental data centre, and other on premises servers similarly were vulnerable to attacks by conventional weapons. Russia also targeted its destructive "wiper" attacks at on-premises computer networks. But Ukraine's government has successfully sustained its civil and military operations by acting quickly to disburse its digital infrastructure into the public cloud, where it has been hosted in data centres across Europe. This has involved urgent and extraordinary steps from across the tech sector, including by Microsoft. While the tech sector's work has been vital, it's also important to think about the longer-lasting lessons that come from these efforts.
II. Second, recent advances in cyber threat intelligence and end-point protection have helped Ukraine withstand a high percentage of destructive Russian cyberattacks. Moreover, the globally interconnected nature of these cyber threat protection solutions means that once threats were identified, organisations across the globe were protected against these threats at machine speed.
III. Finally, the lessons from Ukraine call for a coordinated and comprehensive strategy to strengthen defences against the full range of cyber destructive, espionage, and influence operations.

Today, governments rely on digital communications and data, and one key to sustaining the Ukrainian government has been to disburse these digital operations into the public cloud and outside the country itself.

Prior to the war, Ukraine had a longstanding Data Protection Law prohibiting government authorities from processing and storing data in the public cloud. This meant that the country's public-sector digital infrastructure was run locally on servers physically located within the country's borders. A week before the Russian invasion, the Ukrainian government was running entirely on servers located within government locations that were vulnerable to missile attacks and artillery bombardment. Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, and his colleagues in Parliament recognised the need to address this vulnerability. On February 17, just days before Russian troops invaded, Ukraine's Parliament took action to amend its data protection law to allow government data to move off existing on-premises servers and into the public cloud. This in effect enabled it to "evacuate" critical government data outside the country and into data centres across Europe that are a part of a globally protected ecosystem that includes our full range of security teams.

Technology-based security controls

Given the interconnected nature of IT systems and a threat aperture which is global, threats can come from and target any location. Our view is that the locality of your data in the Microsoft cloud is not considered a security control for data, but rather, is an architectural choice when building applications. In essence, with the correct security controls in place, on the Microsoft Global Network of data centre regions, your data is as secure in a Sydney data centre as it is in Washington, Auckland or Paris Microsoft data centres.

Data location in true hyperscale cloud is an area that is largely still misunderstood in the market, and misconceptions regarding access to data from threats such as insider threat or other considerations such as law enforcement access requests still exist and can inhibit technology adoption. When it comes to data security, in a hyper-scale cloud context, it is important to note that scale, capability, investment and maturity are fundamentally important factors in improving data security.

Global hyperscale cloud providers 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 will fail. Datacentre replication, data mirroring, and other redundancy, failover, and recovery capabilities, used within appropriate geo-boundaries both for the platform and customer transactions and data, are foundational aspects to how Microsoft operates services.

Hyper-scale cloud resiliency also helps customers respond to emergencies and thwart what are traditionally considered extremely difficult to defend against attacks such as 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. Specialised services can also enhance protection.

Microsoft analyses over 65 trillion security signals every 24 hours offering a uniquely comprehensive view of the current state of security and we have more than 8,500 Microsoft security experts from across 77 countries that help to provide a critical perspective on the security landscape. Organisations that effectively manage the lifecycle and flow of their sensitive data as part of their business operations make it that much easier for data security and compliance teams to reduce exposure and manage risk.

Microsoft has estimated that adopting just five best practices would protect against 98 percent of today's attacks:

- enabling multi-factor authentication;
- applying least privilege access;
- keeping devices, infrastructure, and applications up to date and correctly configured;
- utilising anti-malware; and
- protecting data, including by applying sensitivity labels and adopting data loss prevention policies.

Increased international and public-private coordination on developing and disseminating streamlined cyber hygiene guidance could help technology users have greater clarity, prioritise, and act with confidence. As governments around the world increase focus on cybersecurity regulation, ensuring that cyber hygiene practices are in focus will also be important to effectively responding to cybercrime and other threats.

Promotion of software solutions built on global hyperscale cloud providers to small businesses and consumers combined with good cyber hygiene education is one of the most effective ways to quickly uplift cyber security and ensure that Australians have access to world leading technology-based security.

Cyber security and AI

The scale and sophistication of cyber-attacks is rapidly increasing, and the global nature of the threat means that Government's, business and consumers must have access to the most advanced protection capabilities available. The volume and velocity of attacks requires us to continually create new technologies that can tip the scales in favour of defenders. Security professionals are scarce, and we must empower them to disrupt attackers' traditional advantages and drive innovation for their organisations.

Policy and regulatory settings should encourage the deployment of globally competitive advanced hyperscale-cloud based technologies for all Australians from trusted partners. In the last few months, the world has witnessed a wave of innovation as organisations apply advanced AI to new technologies and use cases.

There has long been a perception that attackers have an insurmountable agility advantage. Adversaries with novel attack techniques typically enjoy a comfortable head-start before they are

conclusively detected. Even those using age-old attacks, like weaponising credentials or third-party services, have enjoyed an agility advantage in a world where new platforms are always emerging.

AI has the potential to swing the agility pendulum back in favour of defenders. AI empowers defenders to see, classify and contextualise much more information, much faster than even large teams of security professionals can collectively triage. AI's radical capabilities and speed give defenders the ability to deny attackers their agility advantage.

For example, Microsoft Security Copilot is the first security product to enable defenders to move at the speed and scale of AI. Security Copilot combines this advanced large language model (LLM) with a security-specific model from Microsoft. When Security Copilot receives a prompt from a security professional, it uses the full power of the security-specific model to deploy skills and queries that maximise the value of the latest large language model capabilities. And this is unique to a security use-case. Our cyber-trained model adds a learning system to create and tune new skills. Security Copilot then can help catch what other approaches might miss and augment an analyst's work. In a typical incident, this boost translates into gains in the quality of detection, speed of response and ability to strengthen security posture.

We absolutely believe that security is a partnership, and security should be built with privacy at the core. We build our solutions with security teams in mind— your data is always your data and stays within your control. It is not used to train the foundation AI models, and in fact, it is protected by the most comprehensive enterprise compliance and security controls. While remaining private, each user interaction can be easily shared with other team members to accelerate incident response, collaborate more effectively on complex problems and develop collective skills.

It is important to note that technologies such as LLM AI are computationally intensive capabilities which utilise large amounts of specialised hardware with significant infrastructure requirements. With such a significant investment and substantial ongoing development, it is important to ensure that regulatory frameworks do not accidentally inhibit the use of the latest technology, and as such leave Australia unable to utilise technology which can significantly enhance our ability to protect the nation.

Threat sharing and analysis

Today's cybersecurity threat environment poses a greater challenge than ever before. The sharing of information is a crucial component of collective efforts to defend against and respond to cyber threats, and it is also increasingly expected as an element of organisational cybersecurity risk management programs. However, there are many models for and types of cybersecurity information sharing, and taking steps to effectively operationalise programs and partnerships can be especially challenging.

Information may be shared in one direction or across organisations in either a voluntary or mandatory model. Voluntary, two-way sharing often results in the richest and most valuable exchange, with high trust and impact being foundational to driving collaboration. Increasingly, the reporting of incident information by critical infrastructure organisations is mandatory. As mandatory incident reporting is inherently in one direction and does not, on its own, improve operational security or response, ensuring that requirements are structured to support the reporting of useful information that governments can build the capacity to leverage – and that requirements do not negatively impact incident response – is critical to deriving value.

Enhancing cybersecurity transparency and assurance through certifications and labels

Managing cyber risks is complex, requiring governments, industry, and technology users across the ecosystem to coordinate complementary efforts that contribute to improvements to risk posture. Among other steps, governments can define and implement policies, ICT manufacturers can use a security development lifecycle to develop and maintain products, and technology users can practice good cyber hygiene, such as by using strong authentication and installing security updates.

Microsoft significantly invests in secure product development activities for software, hardware, and services, and we support efforts to provide ICT customers with greater awareness of, transparency into, and assurance of the security practices of ICT providers, including through labelling and certification programs.

While certifications and labels can pose conceptual and operational challenges, such as the need to scale and to ensure customers understand what labels and certifications convey (as well as what their limitations are), an effective approach should help customers make more informed procurement choices.

Cybersecurity certifications and labels should not be perceived as a guarantee against attacks – nor should they be perceived as fully representing the security design principles, capabilities, or features of a product. There are many ways that agile threat actors can compromise products and services, which are increasingly complex, with new security features and functionalities added regularly. In contrast, certifications and labels often focus on a common denominator that is broadly relevant across a range of offerings. As such, they should be considered as part of a broader set of risk management activities that contribute to reducing but do not eliminate cybersecurity risk, and technology users may benefit from additional context on product security differentiators before making purchasing decisions.

Cyber security regulation

As the Government's discussion paper outlines there are a large number of interrelated policies and initiatives that intersect with this strategy development process and wider cyber security regulatory activities. Coordination and alignment to ensure unintended regulatory burden and delays to project timelines can be achieved by using a develop once use many philosophies to key cyber security issues, especially core definitions and international standards.

Any additional proposed regulation or legislation under a proposed Cyber Security Act can be most effective in streamlining regulatory oversight and enabling coordination during an incident. We would recommend that new powers prioritise the ability for the Minister for Home Affairs to coordinate private sector providers and enables agility in response to dynamic threats through risk-based, implementation-agnostic policies that facilitate digital transformation. Today, threat actors rapidly evolve their tactics. Flexible policies that recognise the value of innovation enable technology developers, operators, and users to keep pace with new security capabilities, risk management tactics, and products.

The Australian Government has set a comprehensive security framework for traditional security practices such as physical security and ownership structures, through programs such as the Hosting Certification Framework where we are rated Certified Strategic for Software and a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). We believe that having a coordinated set of clear principles in cyber security that promote proven virtual controls, such as multi-factor authentication and encryption, with international best practice from Government agencies

and service providers is the best method for Government to increase security while ensuring effective service delivery, a reduction in cost and the stimulation of additional growth in the economy.

Cybersecurity policies that are fragmented across technology areas, sectors, and regions risk limiting access to best-in-class security capabilities, undermining the security or functioning of global supply chains, and diverting government and industry security resources towards redundant compliance activities The recent Security of Critical Infrastructure Act (SOCI) process has been a significant development process for cyber security regulation in Australia and Microsoft welcomes the ability to work with both the Department of Home Affairs and the Australian Cyber Security Centre. We would recommend that the Australian Government centralise cyber security policies in the Department of Home Affairs as the central regulator. For example, the Hosting Certification Framework would benefit, through greater alignment, if it was transitioned from the Digital Transformation Agency into the Department of Home Affairs.

A modern cyber partnership

Criminals and criminality cannot be eliminated from cyberspace any more easily than from the real world. They will adapt and change in response to law enforcement and the precautions of individuals and businesses. Nonetheless, by developing a flexible, outcomes-oriented approach to technology, one that takes account of its rapid technical development and the equally rapid evolution of its use, policymakers can insulate from cyber trends as they adapt regulation. Furthermore, by facilitating public-private partnerships with the developers and providers of internet, mobile and cloud technologies, the forces of law and order can stay ahead of the curve; able to spot and jointly emerging criminal trends before they become major threats to businesses, citizens and governments themselves.

The Australian government has a unique place in the economy with the ability to bring a range of private sector partners together to solve problems. Microsoft would welcome a coordinated partnership model with the Australian government, major hyperscale cloud providers, telecommunication providers and key financial bodies such as the big banks. If the government adopts an outcome based collaborative approach to uplifting cybersecurity for small businesses and consumers with a view of increased adoption of modern technologies, then they will significantly increase cyber resilience. Through a process of working with major providers, in these sectors, rapid improvements in technology are possible. We would welcome a structured process facilitated by the department of Home Affairs and led by the Minister for Home Affairs that seeks to uplift cybersecurity through a coordinated private sector and public sector partnership.

We feel the same facilitated process could be adopted to uplift cyber security in the pacific region. Skills, technology adoption, financing and expertise are significant barriers in the region and cannot be addressed by the private or public sectors alone. However, through a coordinated Department of Foreign Affairs and Trade led initiative a comprehensive uplift program is possible. Similarly, to a domestic program this initiative would be best facilitated by being outcomes-based and encouraging the private sector to provide solution ideas to meet the government's problem statement.

Disrupting cybercrime infrastructure

Cybercriminals leverage multiple technology and payment distribution systems to conduct attacks, including websites, servers, email accounts, and cryptocurrency exchanges and wallet service providers. They may manage technology infrastructure themselves or leverage third-party infrastructure, such as cloud services. Disrupting such infrastructure, even when prosecution and arrest are not possible, can impact the profitability of attacks, reversing the incentives and disrupting the supply chains that are contributing to growing threats. Cybercriminals often leverage the same

infrastructure for multiple attacks, but effective disruptions force them to rebuild, adding hurdles and otherwise slowing their pace.

International, public-private cooperation is necessary to effectively disrupt cybercrime infrastructure. The Emotet botnet, which "menaced the internet" for half a decade and supported ransomware distribution, illustrates why. In 2021, in coordination with globally distributed private sector security researchers, a coalition of British, Canadian, Dutch, French, German, Lithuanian, Ukrainian, and U.S. law enforcement not only made arrests but also took down Emotet's "command-and-control" infrastructure (and backups) in more than 90 countries. That level of comprehensiveness, which makes reconstruction of Emotet "seriously difficult," requires cooperation

Microsoft's Digital Crimes Unit (DCU) and security teams are committed to working with ecosystem partners to take down criminal infrastructure through civil legal actions and technical measures. To date, the DCU has disrupted the infrastructure of 25 botnets, preventing them from distributing additional malware, controlling victims' computers, and targeting additional victims. It has partnered with internal security teams to disable Azure infrastructure that was being used by criminals to host malicious software and to notify third-party providers of abuse on their cloud services, enabling them to neutralise malicious activity where it was hosted. And in 2021, DCU directed the removal of more than 596,000 unique phishing URLs and 7,700 phish kits, leading to the identification and closure of over 2,200 malicious email accounts.

We would recommend Government, the private sector, and civil society focus on a collaborative, multistakeholder approach to cybercrime disruption as an important complement to traditional law enforcement objectives and tactics (e.g., indictment and arrest), including by strengthening the partnerships and exchanges that enable coordinated takedowns of cybercrime infrastructure. We would welcome greater structured coordination with the Australian Government and our DCU.

Conclusion

Microsoft commends the Government and expert panel's comprehensive engagement in the development of this paper. We strongly support increased coordination with key cyber security stakeholders to uplift cyber security for small business and consumers. The rapid evolution of technology over the next decade will require a flexible outcomes-based regulatory and policy framework that empowers private/public partnerships and avoids restrictive prohibitions that inhibit Australia accessing new globally competitive technology and techniques as they are made available.