MANDIANT

YOUR CYBERSECURITY ADVANTAGE

Mandiant Response:
2023 – 2030 Australian Cyber Security Strategy Discussion Paper

APRIL 2023

Introduction

The global cybersecurity company, Mandiant, now part of Google, is pleased to present its response to the Australian Government's discussion paper for the *2023-2030 Australian Cyber Security Strategy*. A detailed description of Mandiant can be found in **Appendix A: About Mandiant**.

Over the past several years, the stability of cyberspace throughout Australia's public and private sectors has steadily deteriorated, wherein breaches occur daily and have affected the national conscience in such a way that an enhanced national strategy became a self-evidently necessity in late 2022. A number of endemic causes have led to this deterioration and require acknowledgement to ensure a meaningful and impactful national cybersecurity strategy:

- **Ongoing macro-economic challenges** driven by high inflation, worldwide job security concerns, and the war in Ukraine have led to global uncertainty which suggests cybercrime will likely increase over time, not decrease. Furthermore, defenders of networks will be further challenged as budgets are constrained, causing organisations to prioritise, sustain, and increase cyber budgets during a time of greater fiscal retraction.
- **Inability to hold malicious actors accountable** due to limitations in international legal frameworks and protections provided by some nation states. There are minimal penalties and consequences in place for most financially-motivated threat actors.
- **An enormous increase in the amount and sensitivity of data being collected around the globe**. In the Australian context, a lot of data collection and retention is driven by regulatory requirements and businesses seeking to benefit from data driven innovations.
- **Increasingly complex technical platforms and systems** that are often dependent on legacy technology which are difficult to securely configure and maintain over the long-term.
- **An inadequately staffed cybersecurity workforce** with experienced professionals clustering around the largest and most capable organisations. The cybersecurity workforce is extremely stressed with high burnout rates due to high workloads and severe consequences when incidents occur.

These primary causes directly impact either the likelihood of a successful cyber attack or increases the detrimental consequences following an attack. At a national level, the Strategy must mitigate these primary causes in order for us to see real-world outcomes that we as a nation hope to see, and for which the Government must take the lead.

In addition to several responses to direct questions posed in the discussion paper for the Strategy, Mandiant also respectfully offers its general perspective on two critical components of the proposal – first, related to sovereignty issues, and second, related to the extension of various government authorities.

Sovereign Capability enabled by Trusted Partners

A commitment to "trusted" vendors and partners is necessary to achieve the desired outcomes of the Strategy, whether they are sovereign Australian organisations or based in allied countries. The term "trusted" is relative and should be linked to demonstrated commitment to the shared vision and implementation of a cyber-secure Australia irrespective of nationality and within reasonable scope and consideration to supply chain risks inherent in all nations.

Mandiant observes a significant focus on sovereign-developed cybersecurity capabilities in the Discussion Paper. While we readily welcome improved sovereign capabilities, we caution against the pejorative view that international vendors are inherently negative and should be removed from the Australian cybersecurity ecosystem. Barring overseas based companies from such a key sector in the Australian economy would have cascading negative impacts on the firms and consumers who rely on their state-of-the-art technologies. Such restrictions would impose significant limitations on both the quantity and quality of vendors available to meet the operational needs of Australian governments, businesses, and customers.

Today's cyber threat landscape has moved beyond "one-off" cyber attacks and in most cases involve long-term, persistent campaigns deployed from one nation state against another. Cybersecurity companies – like Mandiant – although headquartered in the U.S., operate worldwide and bring to bear a global perspective that can be effectively applied to Australia's cybersecurity challenges. This is especially important to Australia, its partners and allies as we collectively face unprecedented economic and geopolitical challenges.

The vast majority of cyber capability and infrastructure is incubated, built and sustained overseas. It will take significant time, extending out to at least several decades to develop a comparable indigenous capability, by which time overseas capabilities will also have advanced. An undue focus on Australian sovereign capability at the expense of international platforms and providers will lead to a dip in cybersecurity capabilities and a worsening of the nation's cyber posture.

Australia is presented with an opportunity through our shared democratic values and close existing relationships to enhance our partnerships with key organisations from the United States, United Kingdom and other like minded liberal democracies to enable Australia to set the agenda with these providers and become a true world cyber leader and exporter and implementer of cyber ideas at a global scale. The AUKUS pact in particular presents a unique opportunity to bootstrap advanced Australian cyber capability, and then be both an importer and exporter of advanced cyber ideas and capabilities, through partnership with our closest allies.

As an example of the real world implications of an overly driven sovereign first strategy, prior to the Russian invasion of Ukraine, Ukraine had a national sovereign first strategy for all information services and cyber capability. Barely weeks into the invasion, Ukraine reversed this policy and actively encouraged deploying key Ukraine services into Cloud Services hosted overseas to significantly improve resilience and operational readiness. This decision was arguably one of the most impactful decisions Ukraine took to maintain online services to their citizens amidst an ongoing and sustained campaign by a well-resourced and capable Threat Actor undertaking military operations against their homeland at the same time.

In addition to continuing our ability to provide direct cybersecurity solutions and services to the private and public sectors in Australia, we welcome the opportunity to enhance the nation's sovereign cybersecurity capability through additional training and operational support to build a stronger, more resilient Australian cybersecurity industry.

Extension of Authorities

Mandiant recognises the apparent intention to extend the Australian Cyber Security Centre's (ACSC) authority to interrupt, interject, or otherwise compel organisations experiencing a cyber breach to perform certain actions during a cyber incident, namely to bring under the ACSC's control a major incident, ostensibly only in the event that the victim is unable to manage it independently. However, there are a number of concerns we believe could lead to unintended outcomes:

- The government has not demonstrated why such powers are required. There have been no case studies presented where a lack of authority within ACSC has significantly impacted Australia at a national level. In the most commonly cited recent breaches (Medibank and Optus, 2022) both companies received effective commercial investigative support, in alignment with broader global expectations. What has been reported is the lack of broader coordination extending beyond the immediate technical investigation, which is being addressed with the newly announced National Office of Cybersecurity.

- The ACSC is a part of the Australian Signals Directorate (ASD), an intelligence agency with a primarily foreign signals intelligence remit stretching back over 75 years. The person ultimately responsible for ASD is the Minister for Defence. The increasing scope and power of an intelligence agency controlled by the Department of Defence in the domestic affairs of Australian entities may be perceived as alarming by many Australian citizens.

- ACSC activities are reviewed by the Inspector General of Intelligence and Security (IGIS), with no public or external oversight available to the general public. At a national level, the public will have no ability to review and verify ACSC's activities, and judge for themselves if their activities are appropriate. At a tactical level, the affected organisations will have no authority to question or seek clarifications on the directions received from ACSC beyond that which is volunteered by ACSC. Democratic principles demand public oversight, which can be bypassed by ACSC for reasons that will be opaque to the public. Furthermore ASD and IGIS are both exempt from Freedom of Information requests under FOI Act Section 7 which further impedes the public's ability to determine if ACSC directions are lawful, proportional, appropriate, ethical or in line with democratic principles and Australian public expectations.

- It sends the message that only ACSC has the skills and capabilities to properly manage a major incident. As a commercial Incident Response provider, Mandiant has investigated the largest and most complex incidents around the world. While we acknowledge ACSC's capabilities in this area, we also stand by our own capabilities, and we expect other experienced, capable IR providers do as well. The Government should be seeking to enhance the cyber industry's capability and trust in the market, rather than focusing on an "only government is capable" mentality.

- While Australia's democracy is one of the strongest in the world, there exists significant scope for this legislation to be misused in the future. Legislation must be resilient to misuse not only now, but in the future when different politicians and bureaucrats with unknown agendas are in charge of our most important public entities.

We note that some of the major concerns could be partially mitigated with appropriate guardrails in place. Specifically, placing limitations on the types of activities and requirements ACSC is able to demand, a focus on voluntary partnerships with industry (a carrot) rather than a legislated demand (a stick), and guardrails ensuring ACSC activities are proportional to the incident and the broader strategic context will go some way to addressing these concerns.

A controversial proposition to could potentially address the most extreme concerns raised would be to separate ACSC out from under ASD control. This could include provisioning it as its own Department, Agency or Statutory Authority, to ensure appropriate separation of powers and enabling appropriate public insight into its activities. Maintaining ACSC under ASD, which is Australia's foreign Signals Intelligence (SIGINT) collection and analysis directorate with statutory authority under the Department of Defence, is arguably counter-productive to addressing modern cybersecurity challenges across the nation. Separation would allow ACSC to truly serve as a nationwide cybersecurity authority with a dedicated mission, budget, and workforce to protect all Australian civilian entities from cyber attacks. Additionally, a realignment of civilian and defence cybersecurity missions will comport with public expectations for an open, transparent public institution.

As a SIGINT organisation, operating primarily in a classified environment, ASD unnecessarily restrains ACSC's ability to build rapport with the Australian citizenry and share cyber threat information between the public and private sectors. Furthermore, the current construct does not account for recent market forces wherein the vast majority of cybersecurity capabilities in Australia are developed and retained within industry, which is not dependent on classified SIGINT collection.

We acknowledge this proposition is arguably extreme, and implies its own significant costs in relation to introducing information sharing barriers across SIGINT and cyber defence lines. However it appears to be the most reasonable way to address the significant democratic concerns of the accumulation of domestic power in a Defence controlled intelligence agency, while also addressing external information sharing barriers endemic in an intelligence organisation. We encourage the Government to consider the issues discussed above, and seek to balance those concerns with the legitimate need for the Government, including ACSC, to effectively engage on cyber issues in the future.

Responses to Discussion Paper

Ideas For Inclusion in the Strategy

What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

Thematically we believe the Strategy should espouse the following concepts to be actioned by the Australian government in order to build resilience and ensure its ability to prepare for and respond to cyber attacks:

- Dedicated, long-term funding mechanisms to sustain domestic cybersecurity activities and authorities, relevant law enforcement bodies, and international cybersecurity engagement authorities within Australian government to protect and ensure its cybersecurity capabilities during any future difficult economic climates.

- Incentives to financially support and encourage Australian companies to invest in and protect corporate cybersecurity capabilities.

- A commitment from the Australian government and private sector to endorse an internationally recognised a holistic cybersecurity framework, such as the NIST Cyber Security Framework, to harmonise organisational strategies and establish baselines and benchmarks to improve cyber hygiene.

- Enhanced mechanisms for building resilience across Australia for victims of cybercrime, including modifications to programs that use sensitive or personal identifiable information such as tax file numbers, license numbers, or account IDs. Greater emphasis should be placed on validated recovery options to recover identities and accounts. Furthermore, protections should exist for victims of identity theft, where liability for fraudulent transactions are not passed on to the victim, where credit monitoring services are compelled to protect consumer credit files by default, and where victims are compensated for their time in engaging with service providers. Such a system should be automated in a single online platform, linked to validated MyGovID identities, to automatically trigger rotations of sensitive information and perform notifications to relevant companies, Government departments and agencies and law enforcement where appropriate.

Legislative & Regulatory Reforms

What legislative or regulatory reforms should the Government pursue to enhance cyber resilience across the digital economy?

Mechanisms for reform should encompass a mix of government instruments and policy levers to achieve national cyber resilience. Legislation should be developed and leveraged to establish new authorities or codify existing efforts for civilian and defence agencies with cybersecurity jurisdiction to act appropriately and in a timely manner during attacks. Regulation should be used for critical infrastructure owners and operators to ensure accountability for taking appropriate cybersecurity measures. Any new regulatory activities should be developed with feedback from the private sector and should take existing regulatory requirements into account to ensure harmonisation and avoid duplication. Importantly, any new legislative or regulatory actions should include investments (e.g., funding, technology, and workforce) to allow for proper implementation.

Specific reforms might include clear baseline cybersecurity requirements for critical infrastructure entities to reduce risk and ensure their networks are secured, such as possible enhancements to SOCI legislation. Regulations to establish cybersecurity responsibilities for systemically important entities should be considered and the government should communicate clear guidance to non-critical entities regarding voluntary steps they can take to enhance resilience and better protect themselves against cyber threats.

Finally, enhancing cyber resilience across the digital economy will also require non-authoritative actions as well and require an uplift in the overall cyber literacy of the Australian populace. The government should play an active role in helping all generations understand their cyber footprint and how to reduce the probability of becoming the target of a breach.

Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

Mandiant notes the following concerns regarding the potential expansion of the SOCI Act to include customer data and systems for the following reasons:

- When everything is a priority, nothing is a priority. Including customer data and systems under the SOCI Act provisions will take focus from more nationally important priorities.
- We acknowledge the serious impact on individuals who have had their personal data stolen. However, we believe it is a false equivalency to compare the national impact of the theft and disclosure of personal data to potential negative impacts against utilities such as water, electricity and gas, food supply chains, banking assets, among many other CI categories. Negative impacts against existing SOCI Act categories could lead to death or injury at a national scale; a breakdown of social cohesion and law and order; or the degradation of the financial system, causing a national collapse.
- A key cybersecurity principle is to understand your "crown jewels," and protect the crown jewels first and foremost. A perverse example would be expecting an electricity provider to provide the same level of protection to customer data as they do to their OT network, which provides electricity to hundreds of thousands of people. The consequences of losing electricity, including hospitals, emergency services, banks, supermarkets, traffic lights, public transport (and many other impacts due to a cyber attack) is significantly more profound than that organisation losing customer data due to a cyber attack. Therefore, in this example the electricity provider must prioritise the security and resilience of their electricity production and distribution network by defining an appropriate division of limited funding and resources aligned to the relative risks of the systems. We would still obviously recommend protecting customer data in alignment with the risk profile of the organisation and system, however it should be a lower priority than maintaining the electricity grid.

Mandiant believes protection of personal information (PI) is best viewed in the context of broader national privacy protections. We note the Australian government is currently reviewing the Privacy Act, and that privacy breaches through cybersecurity means should be encompassed within the (assumed) updated Privacy Act. Specifically, the proposed Privacy Act enhancements include provisions to strengthen the requirement for entities to keep personal information secure and destroy or de-identify it when it is no longer needed.[1]

Specific steps that we believe should be taken with respect to PI include (but is not limited to):

- Seek to reduce the amount of PI held by all Australian organisations in alignment with a strengthened Privacy Act where PI data is:
    - Collected for very specific well defined reasons
    - Used in accordance with documented and agreed to uses cases
    - Anonymised whenever possible
    - Discarded as soon as it is no longer useful, and

[1] Privacy Act Report FAQ, 16 February 2023. Retrieved from https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

    - Protected at all stages of the data lifecycle.

- Support Australian industry to become less reliant on PI including, for example, by encouraging commercial adoption of the national identity scheme, MyGovID, for proving identity. Industries that require positive attestation of identity, such as banks and telecommunications providers (among many others), should be able to query MyGovID to determine who a person is, without having to collect and store PI indefinitely.

- PI data management should be regulated and audited, with significant penalties for breaches where data is mishandled (such as allowing a data set to be linked to a person when it can be anonymised), collected for no good reason, or inadvertently leaked. Mandiant assumes that such penalties would be best described in the existing Privacy Act, or future related legislation.

Mandiant notes that the SOCI Act is relatively new, and has not yet formed an opinion on its general effectiveness or where improvements can be made. Furthermore, we acknowledge that many other organisations in Australia may have more relevant experiences and be able to proffer more valuable counsel. Our general perspective is that we need time to adequately measure and assess the effectiveness of the existing regime, before making changes. However, we should not rule out the possibility of changes where those changes are deemed to be necessary for the cyber security of the nation.

Should Australia consider a Cyber Security Act, and what should this include?

Via discussions with The Department of Home Affairs (DHA) and the Expert Advisory Board (EAB), Mandiant understands that the goal and scope of the potential Cyber Security Act (“the proposed Act”) is still under consideration; however, the key driver for the proposed Act is to enshrine in law baseline cyber security obligations across industry and government. There currently exists various cyber security regulatory and legislative requirements that are intertwined or overlap e.g. Privacy Act, SOCI, CPS234. We assume that any consideration of a proposed Act would require a comprehensive review of existing obligations across the economy, and consolidation of obligations into any one proposed Act so as to avoid duplication and confusion in industry. While we offer the following observations, we think it appropriate that any proposed Act be developed in consultation with industry, and designed in a manner that streamlines requirements on entities.

Mandiant supports the development of the proposed Act insomuch as the absence of any single coherent legislation does lead to confusion or willful ignorance about what organisations who otherwise lack the skills, resources or interest to manage cyber risk effectively in a self regulated manner, must do. By enforcing a legally enforced minimum baseline, minimum security standards will rise across the country, especially in low maturity organisations who are not already self governing their cyber programs.

However we caution that the legislation must necessarily tend towards the lower end of the cyber capability spectrum. It is neither realistic or desirable for all organisations to operate to the same risk profile, or chase the highest levels of assurance. Over securitising a platform or organisation on the basis of legislated requirements will negatively impact business innovation, costs, opportunities, efficiencies and effectiveness.

Furthermore, the proposed Act will need to be conscious of avoiding the types of common unintended consequences we often see in regulated industries – specifically, an organisational focus on checkbox security, as opposed to a well considered cyber risk management strategy. We have observed in the past some regulated industries and government organisations so focused on achieving “compliance”, that they will sacrifice overall cyber resilience.

A key topic that was raised by the EAB with Mandiant directly was that the proposed Act may include legislation relating to the provision of cyber security services and platforms, especially in relation to quality and cost of cyber services and platforms. While Mandiant looks forward to further engagement on this topic, our general position is that legislating the cyber industry should again tend towards protecting the lower end of the cyber industry spectrum, and focus on ensuring quality outcomes with quality providers. We do not believe the Government should consider legislating the cost basis of cyber services or platforms as the Government is not best placed to determine an appropriate cost baseline for the industry due to the complex and ever evolving cost dynamics of running a cyber business.

The proposed Act, if enacted, will need to be finely balanced to drive realistic, reasonable cyber outcomes. The scope of the legislation will need to be clearly defined, in consultation with key stakeholders to make it achievable, and above all, effective at improving the nation's cyber resilience. The legislation should be reviewed regularly by both the Government and industry stakeholders, leveraging quantitative measurements of it's effectiveness against clearly defined goals to ensure it is fit for purpose, reasonable and achievable.

How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

Existing regulatory regimes are generally well-aligned to existing priority areas because they are typically aligned to verticals, which organically tend to address cyber risks in a reasonable manner for each of the relevant regulated entities. However, the number of regulatory requirements for businesses has grown over time and in some cases, become duplicative and burdensome, especially when victims are in the midst of managing a cyber incident. Existing regulatory frameworks should be reviewed to harmonise reporting requirements, including to whom, when, and what information is required. Adhering to conflicting or duplicative requirements is time consuming and diverts attention and resources away from incident response efforts. Furthermore, such a harmonisation review should take into account both domestic and international reporting requirements for entities that may be operating outside of Australia in other regions of the world.

Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances? What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

Some governments prohibit ransomware payments to cyber criminals by organisations victimised by ransomware attacks and more broadly financial institutions, cyber insurance firms, and incident response firms. For example, the Office of Foreign Assets and Controls (OFAC) of the U.S. Department of Treasury issued an advisory highlighting that organisations that make payments are not only encouraging future payments but also may risk violating OFAC regulations. Under OFAC, it is illegal to facilitate the payment to individuals, organisations, regimes, and certain countries that are on the sanctions list.

The Australian government should discourage organisations from paying ransoms because there is never a guarantee that stolen data will not be exploited again for further payments. However, at this time a strict prohibition against paying ransomware payments is not advisable. In some cases, victim organisations have immature cybersecurity capabilities and/or lack the resources to properly defend themselves and respond to and recover from a breach. Especially for critical infrastructure entities that provide lifesaving services, such as hospitals or emergency medical or law enforcement response, paying a ransom saves time in getting networks back online and maintaining operations.

That said, Mandiant does not negotiate with threat actors or pay extortion demands on behalf of our clients. Nor do we make recommendations or provide advice on how to respond to such demands. However, we are often asked to help executives and board members evaluate their options with respect to recovering from disruptive intrusions. We advise our clients to discuss with their outside counsel and to think through several considerations before deciding whether or not to comply with extortion demands. We would offer the Australian government the same guidance with respect to making thoughtful choices when considering whether or not to pay a ransom. Some of the considerations are outlined below:

- How quickly can you recover your systems and data on your own? Organisations may not be able to recover their systems and data on their own. This could be due to not having mature backup processes or the threat actor destroying their backups. Often, organisations have good backups, but the restoration process is slow due to the volume of systems that were encrypted and need to be recovered.

- How reliable is the threat actor? Many threat actors recognise their business model requires them to be reliable and credible. If a victim paid a threat actor, and the threat actor did not provide a working decryption tool or published stolen data anyway, the threat actor would develop a negative reputation. This would decrease the likelihood of them being paid by other victims in the future.

- Did the threat actor steal data before they deployed their encryptors? How sensitive is the data that they stole? Recently, most threat actors steal large volumes of sensitive data from victim organisations. Many organisations feel compelled to pay not because they need tools to recover their data, but because they feel obligated to do everything they can to protect their customer and partner data.

- Does the threat actor still have active access to your network? Threat actors almost always establish multiple backdoors into victim environments, enabling them to escalate their attacks if they do not get paid.

- Will cybersecurity insurance cover the claim? Cybersecurity insurance helps many organisations recoup some of the cost associated with the painful decision of paying threat actors.

- Is the threat actor sanctioned by a government agency? For example, paying sanctioned threat actors is illegal in the United States and organisations need to take appropriate actions to ensure that they do not pay a sanctioned entity which could have implications even in Australia. This usually requires support from firms or third party experts and law enforcement.

Proper consideration for a universal ban on ransomware payments should be revisited when there is a greater level of cybersecurity maturity across all sectors. In the meantime, the government should continue a dialogue with the private sector – including victim organisations – to better understand extortion payments and the assumptions about what happens when victim organisations pay threat actors, including several of our observations:

- Threat actors usually deploy multiple backdoors within victim environments. Unless the backdoors are removed and incident containment and remediation steps are taken, the threat actor may have the ability to re-compromise the environment. If a victim chooses to pay the threat actor, they must also take steps to block their access and eradicate them from the environment. This may require investments in cybersecurity tools, processes, and people.

- Many threat actors provide working decryption tools when they are paid. Threat actors realise their business model requires them to provide positive outcomes to victim organisations, or they would develop a negative reputation and they would not be paid in the future. Threat actors often provide decryption tools that work, however, the decryptors often have unintentional bugs that may not effectively decrypt every single file. Because many decryptors are slow and unreliable, sometimes specialised 3rd party decryptors may be used that are faster and more reliable with the decryption key provided by the Threat Actor. But even they are not perfect and are reliant on encryption implementation details that are controlled by the Threat Actor. For these reasons, decryption remains a risky endeavour that may not recover all encrypted files, even if the Threat Actor provides keys and tools as promised.

- Many threat actors do not publish stolen data when they are paid. Some threat actors may provide proof that they discarded the data they stole if they are paid, however, there is no guarantee that the proof was authentic, or they don't have other copies of the data. Prior to 2019, we observed many threat actors that publicised stolen data and re-extorted victims after being paid. Over the next 24 months, Mandiant anticipates some threat actors will re-extort victims and publish stolen data at a later time, despite being paid.

- Many threat actors don't re-compromise entities that paid them. Today, threat actors can opportunistically compromise other organisations easily. They often move on to the next target when they are paid.

Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

The government has a responsibility to Australian citizens to give improved guidance on its expectations in relation to ransomware payments, including the legality of such payments. Mandiant has received feedback from multiple clients that they do not know what their options are with respect to the legality of paying ransoms or any associated reporting obligations for paying a ransom.

Building Regional Resilience with Neighbors

How can Australia, working with our neighbors, build our regional cyber resilience and better respond to cyber incidents?

Mandiant appreciates and often coordinates on cybersecurity matters through the Department of Foreign Affairs (DFAT) Cyber and Critical Tech Cooperation Program but recognises the need for increased regional engagement, including:

- Continued enhancement of regional stakeholder engagement at all levels of government and with private sector entities to educate and seek guidance on issues of most concern to program beneficiaries, including sharing cyber threat information, as appropriate; and raising awareness about long-term, prolific cyber campaigns against nation states.
- More robust, dedicated funding mechanisms – including aid programs – and easily navigable pathways to better support regional allies when under attack by nation states. Commercial providers must have greater access and less barriers to government resources to provide support, especially with respect to liability and insurance concerns.
- A shift towards large scale multi-year, multi-discipline programs of work to build sustained cybersecurity programs and resilience at national or regional scale.
- Increased emphasis on public-private sector partnerships and collaboration, including an exchange of capabilities (and gaps) and requirements and best practices to create greater flexibility for cybersecurity providers to achieve shared goals and objectives and impactful outcomes.
- Alignment with other allied cybersecurity initiatives to ensure effective and efficient programs and to prevent duplication of services, solutions, and support.
- The development and publication of an international engagement strategy and playbook endorsed by regional stakeholders so that partners will know what the priorities are, where their specific project fits into the broader plan, and encourage industry innovation within the broader strategy by highlighting focus areas and program boundaries.
- At an international level, Mandiant expects that DFAT and the Australian Government will continue to make the representations at the appropriate operational, organisational and geopolitical levels in order to create opportunities for ongoing engagement regional engagement.

Opportunities to Elevate International Partnerships

What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Australia enjoys multiple existing international bilateral and multilateral cybersecurity partnerships. The Quadrilateral Security Dialogue (QSD), known as the Quad, a strategic security dialogue between Australia, India, Japan, and the United States; and the defense arrangement between the United States, Australia, and the

United Kingdom, known as AUKUS, are prime examples of Australia and its allies working collaboratively to reinforce norms in cyberspace and think through enforceable mechanisms to collectively prepare for, mitigate against, respond to, and recover from cyber attacks; and importantly, io jointly impose consequences and costs on threat actors. Similar efforts are underway in Australia to specifically address ransomware under the recently announced creation and chairmanship of the International Counter Ransomware Task Force, part of the larger International Counter Ransomware Initiative.

Mandiant is encouraged by these partnerships. However, the Australian government could be doing more, including collaborating more frequently with members of the North Atlantic Treaty Organization and the European Union to better understand and leverage best practices of other multinational bodies on how to collectively defend an entire region against cyber threats. Additionally, the government should consider greater collaboration with other equally cyber-capable nations in the region, including Singapore, Japan, South Korea, and New Zealand, which could become hubs for enhancing cyber capabilities regionally. Such partnerships will be critical to the region in the coming decade.

As Australia considers boosting existing bilateral and multilateral partnerships in the region, the government should also incorporate the private sector into these coordination and collaboration efforts. Employing a “whole of community” approach to cybersecurity is critical to first, obtaining a common threat picture, and second, to preventing, mitigating, responding to, and remediating cyber attacks.

Private cybersecurity providers and governments have distinctive perspectives into the threat landscape, which, when combined, help to form a collective understanding of intelligence. For example, government agencies have the ability to conduct active cyber espionage operations into adversary networks, access network traffic on a national or international scale, or provide additional enrichment through the use of human intelligence sources. There are multiple mechanisms already in place throughout various nation’s governments that perform these types of activities. Conversely, on the industry side, vendors have detailed insight into victims’ networks. Many cybersecurity companies operate on all continents, providing a global vantage point. For example, an endpoint or email protection provider observes a wide and expansive view of the threat landscape. By protecting millions of endpoints, these organisations broadly understand the malware and threat actors that are active within a particular industry or region. Also, incident response firms perform in-depth engagements and build a deep understanding of the attacker lifecycle from start to finish. No single government or private sector company has the best insight. We all have different lenses and perspectives, which means we can learn from each other – a rising tide lifts all boats.

Improved Information Sharing with Industry

What can government do to improve information sharing with industry on cyber threats?

Mandiant encourages the Australian government to consider developing a robust, coordinated structure for sharing cyber threat information with the private sector and vice versa. Such a construct should include sharing information to prevent and mitigate cyber attacks but also to encourage and incentivise private sector entities and government agencies to collaborate and coordinate to respond to and recover from attacks as well. The development of a streamlined sharing apparatus would contribute to Australia’s goals of enabling early detection of malicious cyber attacks and enhancing the government’s situational awareness to better partner with and assist private sector entities that become cyber attack victims. This “whole of community” approach is critical to increasing capacity to prevent and deter future cyber attacks. Sharing information might also include disclosing cyber incidents (which is addressed more fully in a subsequent response to the Strategy).

Key components of a sharing program should include the following:

- Bi-directional sharing – the government must anonymise, contextualise, and in some cases, as appropriate, de-classify cyber threat information and push it back out into the greater cybersecurity community.
- The structure should expand and contract with respect to its membership. Member entities contributing to the sharing program should not be static; commercial providers supporting various sectors should contribute on an as-needed basis to ensure the right entities with the right expertise are participating.

- The government should work closely with commercial providers who might contribute to understand any contractual agreements in place in order to protect customer interests.

There are several benefits for sharing cyber threat information, including disclosing cyber incidents to the government:

- Timely sharing of cyber threat information, within and across sectors, allows for earlier detection of large, sophisticated cyber campaigns that have the potential for significant impacts to critical infrastructure or national security implications.
- Technical indicators, along with contextual information related to attacks, provide a more robust dataset to conduct faster and more accurate attribution and adversary intent. This type of analysis is critical in formulating the most impactful response to such attacks and to do so in a timeframe that has a higher probability of successful countermeasures or deterrence.
- Cyber incident information also allows for cross correlation and collaboration with international partners, thereby enabling a multilateral response to state-sponsored or state-sanctioned cyber criminals that often originate overseas and travel through an allied nation's infrastructure.
- Robust and centralised collection of information provides the government with a much more accurate cyber risk picture and enables more effective and efficient investments and support before, during, and after major cyber attacks.

Confidentiality Obligation for ACSC/ASD

During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

An explicit obligation of confidentiality should be included in any framework for victims to disclose incidents. Creating a safe harbor will incentivise organisations to report incidents and to more broadly share cyber threat information. Liability protections and statutory privilege to not be disclosed in civil litigation should be prioritised when considering legislation or regulation to compel entities to report incidents and share information with regulators.

Expanding Reporting Regime for Cyber Incidents

Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

The Australian government should consider expanding its existing regime for disclosing cybersecurity incidents and evolve it into a mandatory framework. This would improve the general public's understanding of the cyber threat landscape (as appropriate, when the government makes public announcements detailing attacks) but more importantly improve the overall cybersecurity posture of every critical infrastructure sector and governmental organisations at all levels. Generally, major tenets of such a program should:

- Safeguard the protection and integrity of electronic and other types of data
- Ensure confidential sharing
- Encourage entities to adopt recognised cybersecurity standards and practices with a minimum threshold
- Provide greater incentives for private sector entities, including liability protections and statutory privilege to not be disclosed in civil litigation (e.g., confidentiality obligations)

- Protect privacy and civil rights
- Provide outreach and technical assistance to entities that do not have cybersecurity expertise or capabilities
- Define “security incidents” for reporting to focus more on the attacks on IT systems that compromise the product development, build and visibility environment
- Ensure thresholds for reporting meet capacity – must have the proper infrastructure and workforce in place to consume, enrich, and share data back into the security community (high reporting volumes of low-severity incidents undermines critical cybersecurity support needed to actually respond to incidents)

Mandiant believes that strong cyber community protection is predicated on several key concepts. The Australian government should consider the following additional components that we believe would constitute a robust and ultimately successful cyber incident reporting program:

Establish reasonable and effective timelines for reporting

- Reporting requirements should account for two key outcomes: 1) timely and relevant reporting of critical intelligence to relevant government authorities for assessment, correlation, and decision support; and 2) reasonable latitude for the victim to determine the nature, extent, and potential impact of a breach. In the first instance, the timeliness and quality of the data reported to the government will largely determine how effective the response to and disruption of the attack will be. In the second instance, cyber attacks are often complex and require sophisticated analysis to understand the full scope of compromise.
- Victims require support from external firms to fully analyse a breach and will likely be dealing with other business impacts and crisis management activities. Allowing for a reasonable amount of time to properly assess the situation before requiring reporting will limit false positives, redundant or contradictory information and prevent unnecessary data collection.
- The government should consider harmonising reporting requirements with existing requirements, regulations, and standards (both domestic and in other countries where commercial providers may be conducting business) to provide for a consistent and streamlined regime that simplifies business processes and compliance and reduces the burden on victims.

Preserve existing trusted relationships and partnerships

- Mandiant strongly believes in the concept of a public-private partner approach to cyber security. Unlike most other domains of risk, cyber attacks and cyber crime are almost always predicated on the use, traversal, or compromise of privately owned infrastructure, even when the attacks are focused on government or national security assets. The private sector, especially critical infrastructure sector businesses, is both a key component of overall national cyber resiliency and a key source of intelligence on our adversaries’ capabilities, intents, and activities in cyberspace.
- Over the past decade, many Australian government agencies have built partnerships with key cyber security and critical infrastructure organisations through voluntary programs, outreach, and support. While we recognise that much more needs to be done, without these efforts and support functions, many private sector cyber attacks would have likely remained undetected for much longer and would have been much more severe. Under a new cyber incident reporting program, these trusted relationships and partnerships must be strengthened and enhanced to advance our common goals of reducing the frequency and severity of cyber attacks.

Ensure compliance is non-punitive

- A reporting program must encourage cooperation and strengthen trust between the public and private sector. A regulatory-based approach or a regime that focuses on punitive actions rather than mutual benefits would be counter to the goal of creating a strong national partnership model to counter the increasing cyber threats we are facing.

- As previously suggested, although mandatory reporting is necessary, the focus should be on supporting organisations to achieve compliance, not punishment for non-compliance. Fines and other financial or legal punishments do not properly reflect the truth that, barring gross negligence or willful misconduct, organisations that suffer a cyber attack are victims of a crime. Mechanisms to compel collection of critical information when necessary, such as subpoenas, better align to the general concept of criminal investigation and response.

Require information to flow back into the community

- Information sharing must be bi-directional. An incident reporting framework should allow for a consistent flow of two-way information sharing between the public and private sectors to help maximise the ability to resolve and consider attribution.
- Organisations that invest significant effort into collecting, analysing, and sharing cyber attack technical information require feedback on the usefulness and value of what they have provided. They also benefit from data that can only be provided by the government to enhance their own security posture and help to hone their threat detection and response functions.

Automated Threat Blocking at Scale

What best practice models are available for automated threat-blocking at scale?

Mandiant encourages the Australian Government to consider three key principles related to large scale, national level threat detection and blocking: Authorities, Visibility, and Applied Intelligence. First, as part of a strategy for automated, large scale threat blocking, the government must consider relevant authorities to either directly collect and analyse cyber threat relevant data or collaborate with private sector information and telecommunications providers to gain real time visibility into network telemetry. These authorities can exist in a two-tiered approach. Tier one would consist of “peace time” or standard threat level operations and Tier two would consider an elevated or exigent threat level that requires a higher posture of threat detection and blocking.

Second, visibility in the context of national level cyber threat detection and blocking consists of national level gateways and other external (North / South) gateways and boundary networks, as well as key internal (East / West) network segments. At each of those visibility layers, general and focused detection and blocking can be implemented. General detection consists of protocol analysis and can include capabilities such as:

- NetFlow traffic analysis
- DNS protocol analysis
- Remote access and VPN protocol analysis

General analysis can also include behavioral analytic capabilities such as:

- Correlation to know bad traffic patterns
- Correlation to other current / ongoing cyber attacks
- Heuristic, pattern, and geolocation analysis

Focused detection and blocking is usually implemented at the heightened security posture level or within specific sectors that are systemically important or at high risk based on current threat information. These capabilities tend to be more intrusive and / or impactful to normal operations and therefore usually require additional authorities and justification to invoke. Examples of focused protocol and behaviour analysis

- Full packet capture
- TLS break and inspect

- DNS intercept and blackholing
- Attachment and payload reconstruction

Finally, the scalability and automation of these capabilities relies on robust, accurate, and actionable threat intelligence data. Cyber threat tools, techniques, procedures, and indicators must be applied at both the general and focused levels to effectively identify, correlate, and block malicious content and adversarial actions. Consideration should be given to implementation of cyber threat intel sources that include private sector and vendors as well as more sensitive government intelligence sources.

Government Response to Major Cyber Incidents

How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

Beyond establishing new legislation or regulation and taking into account existing structures for law enforcement, sharing cyber threat information, and responding operationally to attacks, the Australian government should consider establishing a centralised office to coordinate its processes and policies for securing the nation against cyber attacks. For example, the United States created an Office of the National Cyber Director (ONCD) in 2021 with congressional action and White House endorsement following the Solar Winds incident. There was a recognition that a coordinated office and dedicated workforce within the Administration was required to improve the overall cybersecurity posture of the U.S. The Director advises the President on cybersecurity strategy and policy and coordinates activities across the federal government/interagency, state and local governments, industry, and academia to develop sound cybersecurity policies.

Mandiant is pleased to note the recently publicised establishment of the National Office of Cybersecurity, headed up by the National Cyber Coordinator. We assume this office will become the nexus point for national coordination of cyber incidents in the future, and we look forward to working with the office in a positive and meaningful manner.

Should Government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Harmonising reporting requirements and establishing a single reporting portal for cyber incidents would lessen the burden for victims when experiencing an attack. Mandiant supports the development of a single reporting portal with automated routing of notifications for victims of cyber incidents. Agencies that often have conflicting timelines or different reporting requirements add an unnecessary layer of complexity to the incident reporting and response processes. We regularly receive feedback from victims that there is uncertainty with respect to whom, when, and for what purpose they are reporting an incident, oftentimes diverting critical resources to responding to, investigating, and recovering from an attack. A single portal will make reporting significantly easier for victims when they need it most and improving outcomes for the victims of a cyber incident. It will also ensure consistency of the information being shared.

Opportunities to Enhance Australia’s Cyber Security Technologies Ecosystem

What opportunities are available for government to enhance Australia’s cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Mandiant fully supports the intention to uplift Australia’s cyber security services and technologies ecosystem. Our focus is on building trusted partnerships with some of Australia’s most capable existing and emerging cyber companies, and we look forward to supporting the Australian cyber industry in the years to come.

The government should consider emulating models for uplifting the security of Australia’s industrial base, for example, considering such concepts as “secure by design” or “secure by default” – baking security into the development of products rather than bolting it on later once products have entered the market and become more vulnerable as they move through the supply chain and/or consumed.

For example, the latest national cybersecurity strategy from the United States acknowledges both the complexity of the global, interconnected, digital ecosystem as well as the crucial nature of public-private cooperation to secure that ecosystem. Thematically, the U.S. strategy seeks to correct market failures to foster a trustworthy system and surmises that government intervention is required to raise the level of security across critical infrastructure and the broader technology ecosystem. In theory, this would remove the burden of security from the users and shift some of the responsibility to developers, and more generally, to larger entities that can manage concentrated risk and more reasonably shoulder the burden from a resource perspective. The overall goal of this concept is to assist “resource-poor, target-rich” businesses to drive resiliency across the nation. Specific actions associated with this concept could include legislation to establish liability for software, incentives for companies who build products which are secure by design, or a voluntary labeling scheme for consumer IoT devices.

Opportunities to Use Procurement to Support and Encourage Australian Cyber Ecosystem

Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

We believe procurement levers can be used to improve cybersecurity resilience, specifically in relation to building cybersecurity requirements into all technology procurements. Each procurement owner must give due consideration to the protection of the system being procured, fast detection of incidents within the system and recovery of the system if it is compromised, in alignment with organisational risk profiles and industry best practice. Such levers should encompass build and sustain phases of the project, and cover people, process and technology. For example, project requirements could state that; 1) the system must be aligned to NIST SP 800 series of frameworks, 2) it must integrate with existing security operations tooling and 3) the system must integrate with the organisations existing Incident Response Plan.

We encourage viewing international vendors as key elements in Australia’s cybersecurity ecosystem, bringing global perspectives and experience which can be leveraged by Australian cyber security firms to improve outcomes for all Australian organisations. We believe procurement barriers that isolate and denigrate international vendors will have the reverse effect and will lead to worse cyber outcomes for the nation.

Final Commentary

Mandiant thanks the Australian Government including the Minister for Cyber Security, the Shadow Minister for Cyber Security, the Australian Cyber Security Strategy Expert Advisory Board, the Department of Home Affairs, the Australian Cyber Security Centre and the Department of Foreign Affairs and Trade for the opportunity to meaningfully engage in the development of the 2023 – 2030 Australian Cyber Security Strategy.

As a global cybersecurity vendor, we have been fighting the good cyber for nearly 20 years, and we are committed to continuing the fight for the next 20 years and beyond. We look forward to working with the Australian Government to ensure the 2023 – 2030 Australian Cyber Security Strategy delivers on its goal of making Australia one of the most resilient cyber nations in the world.

Appendix A: About Mandiant

Founded by Kevin Mandia in 2004, Mandiant is a pioneer in educating organisations and governments around the world about how to secure their networks against advanced targeted attacks and providing security consulting and incident response services to help them resolve security incidents, when they occur. As a trusted security advisor to more than 75% of the Fortune 100 and companies of all sizes, Mandiant consultants have responded to some of the most high-profile security incidents and supported organisations around the world with expertise to measure, optimise and continuously improve security programs. The company has driven intruders out of the computer networks and endpoints of hundreds of customers across every major industry.

Our mission is to relentlessly protect security-conscious organisations and critical infrastructure with innovative technology and expertise gained from the frontlines of incident response, advancing every security team in the world regardless of the security controls they have deployed. To accomplish its mission Mandiant has attracted the leading cybersecurity practitioners, experts, and analysts in the world. Mandiant consultants have published experts, speakers at well-known security conferences and experts sought by leading media organisations. Mandiant employs former law enforcement officers, intelligence officers, Department of Defense computer security specialist, and forensic examiners who have significant experience shaping the information security programs at large complex organisations. Our expertise is complemented by an extensive infrastructure of patent-pending technology that Mandiant has developed to proactively detect and respond to advanced threats at scale within an enterprise. Mandiant is a CREST STAR accredited member company for Intelligence-Led Penetration Testing. https://service-selection-platform.crest-approved.org/member_companies/mandiant-consulting/

Since 2004, our industry-recognised threat researchers, reverse engineers, intelligence analysts and incident responders have been live on the frontlines of cyber conflict. We now have consultants placed in 26 countries, assisting organisations with their security needs. Mandiant has a uniquely dynamic view of the attack lifecycle, combining machine intelligence, adversary intelligence and operational intelligence to form the most comprehensive library of threat actor activity available.

On September 12, 2022, Google LLC   announced the completion of its acquisition of Mandiant, Inc. Mandiant will join Google Cloud and retain the Mandiant brand. With this acquisition, Google Cloud and Mandiant will deliver an end-to-end security operations suite with even greater capabilities to support customers across their cloud and on-premises environments.

More Information: https://www.mandiant.com/

Report an incident: https://www.mandiant.com/report-incident