Search. Observe. Protect.

Submission for the 2023-2030 Australian Cyber Security Strategy Discussion Paper

Asjad Athick

Lead Security Specialist - APAC, Elastic

elastic.co

Executive Summary

Elastic welcomes the opportunity to participate in Australia's 2023-2030 Cyber Security Strategy development process. The COVID-19 pandemic has rapidly accelerated the adoption of digital technologies, making Australia a prominent target for cybercrime. This shift has led to significant cyber attacks, including unprecedented data breaches impacting major publicly listed companies with substantial knock on effects to the economy and the community. According to the Australian Cyber Security Centre's 2021-2022 threat report, there is a cyber incident every seven minutes. However, the cyber sector offers significant opportunities for Australia's digital economy, and the government should position to harness this potential for a prosperous future.

We commend the government and Cyber Security Minister Clare O'Neil for the initiative to transform Australia into the most cyber secure nation by 2030. We believe that a whole-of-nation approach is necessary to keep our critical data, systems, and infrastructure safe. Focus should also be on ensuring the right legal and policies are in place to keep pace with the challenges presented by the digital world. It is essential to approach this with an open and transparent mindset, enabling cost-effective and agile capabilities (in terms of people, process and technology) to be easily adopted and reused across the economy. Cyber criminals are highly organised and coordinated. Our defensive capabilities must be too.

To address the emerging cyber security threats in the digital economy, Australia's Cyber Security Strategy should promote security by design in new technologies. It is critical to prioritise security during the development of new technologies, ensuring they have a built-in security framework that meets the highest standards. This approach can reduce the potential vulnerabilities and minimise the risks posed by emerging technologies. At the same time, it is important to design resilient systems that can survive breaches, with minimal impact to citizens. Security incidents can sometimes be inevitable, even on the most hardened and secure systems. It is important for organisations to invest in capability to quickly respond and contain breaches, while communicating clearly and transparently with stakeholders.

Moreover, the Cyber Security Strategy should focus on building a skilled and capable workforce to combat cyber threats. The government should invest in the development of programs and initiatives to promote cyber security as a career option and provide training and certification for professionals. This will help ensure that the workforce is equipped with the knowledge and skills needed to address the growing cyber threats in the digital economy.

In conclusion, Elastic believes that the Cyber Security Strategy should prioritise a whole-of-nation approach, promote security by design in new technologies, and focus on building a skilled and capable workforce to combat cyber threats. With these initiatives, Australia can achieve its goal of becoming the most cyber secure nation by 2030.

About Elastic

Elastic Security is focused on helping organisations detect, prevent and respond to cyber threats across their on-premise and cloud environment, by taking an open and transparent approach to security. Built on Elasticsearch, the most popular open-source search and analytics platform, Elastic Security provides SIEM, Endpoint Security and Cloud Security solutions on one unified platform.

With Elastic, organisations can build in-depth security visibility into their environment, giving teams the ability to quickly search, detect, contextualise and remediate threats before the business is impacted.

Elastic's works with organisations of all sizes, from startups/scaleups, to financial institutions, government agencies and critical infrastructure providers. With widespread adoption of our solution, Elastic was recently named a Leader in the Forrester Wave for Security Analytics platforms.

About the author

Asjad Athick is the Lead Security Specialist for APAC at Elastic with 10+ years of experience in building security operations capability. He specialises in cloud-native security and vulnerability management and is passionate about empowering security teams with the tools they need to keep their organisations safe. Asjad is a thought leader in the cybersecurity community and a frequent speaker at industry events across Australia and the APAC region.

Please contact either Asjad Athick [redacted], or Anna Mascarello, Vice President for Public Sector, Australia [redacted] for more information about Elastic or the contents of this submission.

Elastic's Response

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

The strategy to make Australia the most cyber secure nation in the world should be based on core pillars including:

- Cyber resilience
    - Develop clear and practical guidelines, resources, and tools to assist small to medium-sized businesses in implementing effective cybersecurity controls.
    - Modernise the Essential 8 framework to align with changing environments and workloads (such as cloud native environments, significant usage of SaaS services, third party vendors etc.).
    - Define and communicate minimum recommended cybersecurity capabilities and controls for large enterprise organisations.
    - Advocate for increased adoption of the Australian Government's Information Security Manual (ISM) or higher maturity compliance of Essential 8 across government agencies.
    - Simplify integration and lower the barrier to entry for business to integrate with productized document and ID verification services to reduce complexity and costs, while preserving privacy.
- National digital infrastructure
    - Actionable threat intelligence consolidation and sharing services
    - Build and expand document verification services to include biometric identification for enhanced security and fraud prevention.
    - Elevate national ID security and fraud standards to bolster trust and confidence in government services, while limiting the impact and blast radius of a successful breach.
- Nurturing industry and developing an export market
    - Offer favourable tax incentives and grants to incentivize the growth and development of the cyber products and services sector.

    - Provide access to government procurement opportunities to enable startups and small businesses to compete with larger players in the market.
    - Promote international trade and exports by facilitating access to international markets and promoting Australian cybersecurity products and services globally.
    - Foster collaboration between government and industry to identify emerging market opportunities and align resources to take advantage of them.
    - Encourage partnerships between industry and academia to support research and development, and to ensure a pipeline of skilled talent for the industry.
    - Leverage Australia's unique strengths, such as its proximity to Asia, to position itself as a leader in the Asia-Pacific cybersecurity market.
    - Consider other high tech, competitive economies in Asia and Americas with better business environments, that companies would move to.
    - Stay up-to-date with emerging trends and technologies to remain competitive with other high-tech economies in Asia and the Americas.
- Strengthening the ecosystem
    - Adopt open and vendor-neutral security strategies across government organisations to facilitate interoperability and avoid vendor lock-in.
    - Apply competitive and transparent procurement strategies to modernise systems and promote innovation.
    - Conduct thorough market evaluations of products and services to inform purchasing decisions.
    - Emphasise process, methodology, and outcomes over technology to encourage competition and innovation.
    - Strengthen the overall Australian cybersecurity ecosystem through collaboration and information sharing between government, industry, and academia.

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

- Streamline and simplify the reporting requirements for cybersecurity incidents across various current obligations, such as the Privacy Act, Security of Critical Infrastructure (SOCI) regulations, and Australian Securities Exchange (ASX) rules.

- Mandate baseline cybersecurity standards for critical infrastructure providers and key industries, such as finance and healthcare, to improve their resilience to cyber threats.
- Establish a framework for the secure sharing of threat intelligence between government agencies, industry, and academia to improve situational awareness and response capabilities.
- Develop a clear and consistent regulatory approach to emerging technologies such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain to ensure security and privacy by design.
- Promote cybersecurity awareness and education initiatives to increase the cybersecurity skills and knowledge of individuals and businesses.
- Encourage the development and adoption of international cybersecurity standards, such as the ISO 27001 and NIST Cybersecurity Framework, to enable interoperability and enhance cybersecurity best practices.
- Increase regulatory oversight and enforcement to ensure that businesses and organisations are meeting their cybersecurity obligations and to deter cybercrime.

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

Regulations and regulatory guidance play a critical role in ensuring compliance with mandatory operational cybersecurity standards established by legislation. Regulators can provide specific requirements and guidelines for companies to follow, and monitor and enforce compliance. Regulatory guidance can also offer additional clarification and advice on how companies can meet the mandatory operational cybersecurity standards. This can include best practices, case studies, and other resources to help companies understand and implement the standards effectively. By providing clear and specific guidance, regulators can support companies in meeting their obligations and help to ensure a consistent and effective approach to cybersecurity across industries.

b. 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?

When considering data protection and privacy reforms, it is essential to consider the value of defining customer data and systems across all sectors of the economy. While SOCI enforced sectors may hold sensitive customer data, it is crucial to recognize that similar data may also be held by small and medium-sized businesses and enterprises. Any reform around data protection, identity, and privacy must be applied across the entire economy, rather than being limited to particular sectors. By taking an economy-wide approach to data protection, privacy, and security, we can ensure that all businesses and organisations are held to the same high standards, and that customer data is protected consistently, regardless of where it is held.

c. Should the obligations of company directors specifically address cyber security risks and consequences?

Cybersecurity risks pose a significant threat to companies, leading to financial losses, reputational damage, and legal liability. Company directors have a legal obligation to act in the best interests of the company, including managing risks that may impact the company's operations, reputation, and financial position.

However, cybersecurity risks are becoming increasingly complex, and many directors may lack the necessary expertise to fully understand these risks. Therefore, it is crucial that directors receive appropriate training and resources to understand these risks and the measures needed to mitigate them.

By incorporating cybersecurity risks into the obligations of company directors, companies can take a proactive approach to cybersecurity and reduce the risk of cyber incidents. This approach will help protect the interests of stakeholders, including customers, employees, and shareholders, and safeguard the long-term success of the company. Directors must recognize the critical role they play in ensuring the security and resilience of their organisation's digital infrastructure, and must take an active role in managing cybersecurity risks.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:

(a) victims of cybercrime; and/or

Paying ransoms and extortion demands can incentivize cybercriminals to continue their illegal activities, as it provides them with a financial reward for their actions. This can also lead to a cycle of escalating demands, as cybercriminals realise that victims are willing to pay to recover their data or systems. By prohibiting payments, the market for criminals will substantially shrink, resulting in less persistent targeting by criminals. Furthermore, a large number of victims that pay ransom do not successfully recover their systems. The industry has also seen a trend globally indicating more and more victims are opting not to pay ransoms and recover systems from backups etc.

An exceptions/review process could be considered in rare cases where paying a ransom outweighs the loss to a business or the australian economy

(b) insurers? If so, under what circumstances?

Assuming victims are prohibited from paying ransoms, insurers should be prohibited from doing the same. Appropriate grace periods should be issued, to allow organisations to consider their risk posture, and insurance policies. Ultimately, reducing the amount of payments made to ransomware operators reduces the level of investment from their end, while forcing businesses to uplevel their security posture.

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

Victims, companies and insurers will face short term difficulties as they manage data loss etc. but will lead to positive long term effects by reducing the prevalence of ransomware related crime. Various free and open source security tools such as Elastic Endpoint Security exist that companies can leverage and apply as controls to reduce the impact of ransomware long term.

Resources that further elaborate Elastic's stance on the matter:

- Why the best kind of cybersecurity is Open Security

- Open source Endpoint and Cloud security

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

Yes. Many businesses look to clear government advice on the matter.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

- Adopt cybersecurity compliance frameworks like the ISM and demonstrate a strong, continuous, and incrementally increasing compliance posture across all capabilities.
- Establish regular knowledge-sharing cadences and communities of practice across groups of agencies, with industry participation to uplevel everyone involved.
- Demonstrate security thought leadership through conference talks, whitepapers, and other mediums to share knowledge and experience with others.
- Highlight the unique challenges, opportunities, and solutions present to drive knowledge sharing and promote awareness across departments and agencies.
- Look beyond compliance regimes and chart a path towards complete defence-in-depth ways of securing environments.
- Openly communicate milestones, achievements, and successful security programs to showcase the effectiveness of cybersecurity best practices and inspire others to adopt similar measures.

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

The government can maintain an information sharing and dissemination platform that collates key indicators of compromise and tactics and techniques that can be turned into actionable intelligence in common security platforms and tools. While the ACSC reports contain some of this information, it is difficult to automate and deploy at scale across enterprises. By providing a centralised platform, the

government can facilitate information sharing with industry and improve the effectiveness of their cybersecurity strategies.

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

Automated threat-blocking at scale can be achieved through various best practice models such as Endpoint Detection & Response (EDR) and Network Detection & Response (NDR) tools. These capabilities rely on global threat research conducted by vendors and research communities to proactively block threats before they cause harm. It is essential to invest in these preventative measures for effective security.

However, in cases where automated threat-blocking is not feasible, it is crucial to assume that all systems may be breached someday. Therefore, investment in the ability to quickly respond and contain the threat is equally important. One approach to achieving this at scale is to invest in core capabilities such as centralised logging and monitoring for security analytics, also known as SIEM platforms. Modern cyber security detection and investigation capabilities boil down to the level of visibility organisations have into their environment, making security a data problem.

By creating and sharing SIEM detection rules in a timely manner, organisations can quickly deploy additional detections to identify, investigate, and hunt for indicators in the event of a breach. These detection rules can be based on common schemas, open source/industry-standard languages, and tools to facilitate efficient and effective threat detection and response.

To achieve this outcome in the industry, Elastic publishes and maintains all it's SIEM detection rules for anyone to adapt and consume for free.

