Submission to Australian Government

2023-2030 Australian Cyber Security Strategy Discussion Paper

Genetec Inc. is pleased to provide the following response. This submission specifically targets cybersecurity concerns related to physical security solutions. As IT and physical security technology have converged, new potential threats have emerged that the government should understand and address as part of its policy.

NOTE: Only questions related to these points of convergence are addressed in this submission:

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?

For Australia to meet its vision of being the world's most cyber secure country by 2030, the government needs to place focus on technologies that are critical to cyber resilience, increase the maturity posture of its IT (information technology) and OT (operational technology) systems, and limit its reliance on technologies that are developed by foreign government owned companies from countries that do not share Australian values and principles related to human rights, individual privacy and cybersecurity. In addition, it is critical that government officials be well-versed in risk assessment which includes understanding threats posed to the country when procurement supply chains are not fully evaluated and when price is the main deciding factor in the purchase of technology.

Internet of things

Government organisations, schools, higher education, critical infrastructure, and healthcare institutions can all be vulnerable to a disruptive and costly cyber-attacks. While we typically think of computers as primary targets of attacks, any internet connected device can be the source of a cyber-breach. Physical security hardware, such as surveillance cameras and access control readers, are modern internet protocol (IP) devices which are essentially sophisticated computers with privileged network access. This means hacking into one of these devices could potentially put the government network at risk. Although surveillance cameras represent just 1.2% of all internet connected devices it is critical to understand that they account for 24% of malicious activity.

Still, many government (and private) organisations lack the knowledge needed to select a truly compliant and cyber-hardened technology. And because of budget constraints, they may select cheaper options that also claim to be cyber-resilient but may pose significant risks to their network.

Only by putting in place stringent evaluation processes at every stage of the supply chain will Australia be able to root out attempts by foreign adversaries to exploit vulnerabilities that could lead to intellectual property theft, software corruption, attacks on critical infrastructure, and more.

Partnering with the private sector

Bolstering cyber resilience and protection requires a multi-pronged strategy that involves a much deeper level of coordination and partnership between government and the private sector. A top priority should be protecting and ensuring Australia's critical infrastructure which is mostly run by the private sector. For their part, businesses should document cyber incidents and threats, share that information with their government partners, and proactively communicate with their supply chains, customers, and other stakeholders in a timely manner to maintain their reputations and to protect all parties involved.

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

Technology that is produced and distributed by companies owned (in whole or in part) by foreign governments that have a strategic interest in exfiltrating data, intelligence, or intellectual property from rival governments, private businesses, and individuals comes with significant risks. This is especially true when the country and/or companies in question have demonstrated a lack of responsiveness and transparency related to proven, documented issues related to their cyber security policies and/or track record. Understanding the inherent risks of working with these organisations and their technology must be clarified to policy makers and they should be excluded from participating on government projects - even if they appear to have a lower price. In the long run, acquisition of this technology could cost the country much more in terms of both cyber risk and potential need to rip out and replace hardware found to be easily exploited once deployed.

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

Australia has taken a significant first step with the federal and local governments and military removing state-owned camera manufacturer products from all its agencies over national security concerns. As a leading voice in the APAC region, Australia could encourage its neighbours and trading partners to follow suit.

Perhaps a next step for Australia would be to legislate against the use of these devices in private businesses, especially those involved in critical infrastructure serving the nation. Such a step is not unheard of – the United States evaluated the risk to be too high for such devices and banned them outright in both public and private organisations (US NDAA ban 2018, and US FCC ban 2022).

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

As the world has become increasingly interconnected through the move to cloud computing and Internet of Things (IoT) devices, cyber-crime has risen steadily, along with tools to combat it. However, geopolitical tensions between countries have the potential to rapidly unleash devastating cyberattacks worldwide, escalating the need to be cyber aware. To mitigate this risk, it is essential to reinforce core alliances with allies and strategic trade partners while working with international industry and global technical standards bodies. As conflicts continue and geopolitical tensions rise, especially in the Asia Pacific region, public and private sector organisations must work together and remain vigilant for malicious cyber activity targeting their networks. Borders do not exist in cyberspace and once malware is deployed it can infect vulnerable systems worldwide.

It's also critical for Australia's government organisations to carefully select vendors to supply projects that maintain compliance with cyber security standards to ensure products are cyber hardened.

Another recommendation would be to align on certifications, favouring well established international standards, and a requirement for vendor technology to comply/adhere to these certifications.

The government should be aware and select standards as guidelines and baselines for best practice. These may vary depending on the project at hand but could include ISO, IEC, industry association standards, or a choice of regional standards. Some are general-purpose IT cyber standards (like ISO 27000 standards), and, in the case of physical security technology, some are specific to life safety and security systems (IRAP, CAPSS, UL 2900-2-3).

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

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

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

8. 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?

9. 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?

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

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

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

14. What would an effective post-incident review and consequence management model with industry involve?

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

16. 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?

It is fundamental for Australia to select trusted partners and vendors. Ones that are not only focused on mitigating present vulnerabilities and future risks but who also maintain cyber security at every stage of their supply chain. It's important to note that the past actions of these partners/vendors are a clear indication of potential future behaviour and support.

The impact of just one weak link in Australia's technology supply chain can be significant. A single incident can lead to operational disruptions, compromised data, and more. To hold their supply chain partners, and themselves, to higher standards, Australia's government organisations need to carefully evaluate which vendors have access to their network. They must be explicit about ethical practices and security requirements in their contracts, carefully monitor their technology providers and other partners, and seek constant improvement. Failing this, the government could risk undermining the trust upon which growth, prosperity, national security, and international relations rest.

To make informed choices, here are some of the questions that should be asked:

- Does the vendor proactively monitor the emergence of new threats and their potential impact on operations, data, and people? Do they have a comprehensive strategy in place to close security gaps and vulnerabilities? What policies do they have in place concerning cybersecurity?
- Are their solutions developed with a defence in depth approach, with several security layers such as employing advanced authentication and encryption technologies? Are they protecting the organisation's data and the privacy of their customers?
- Do they work with partners who also have security and data protection in mind? Do they carefully vet and select the partners to ensure the highest levels of cybersecurity and compliance?
- What measures do they take to inform and support their customers regarding cybersecurity best practices? Are they forthcoming about known vulnerabilities and do they share strategies and fixes for quick remediation?
- Data security and privacy standards: Do they adhere to information security standards such as ISO27001? Do they engage third-party auditors and conduct penetration tests to identify and address security gaps? Do they have any certifications from other regulatory bodies and international associations?
- Is the technology banned or in the process of being banned by significant allies of Australia such as the United States of America, or the United Kingdom?

17. How should we approach future proofing for cyber security technologies out to 2030?

Prioritising cybersecurity is key and it's necessary to put in best practises to help limit the likelihood of hackers breaching products. There is no single silver bullet when it comes to security, so organisations need to put in place controls to better detect breaches, mitigate their scope, or prevent them altogether, including but not limited to:

- Multi-factor authentication, which helps prevent threat actors from login in using solely the username and password combo that could be harvested through phishing or previous breaches.
- Segregation of duty: by ensuring that privileged accounts are few, tightly controlled, only used for their intended purpose, and adhering to the principle of least privilege.
- Monitoring of IOCs (Indicators of Compromise): monitoring events such as 'impossible travel' would allow for earlier detection of these breaches.
- Security/Privacy by design: Ensuring that administrators of the system cannot easily access customer data without explicit consent by users, ensuring the data is not accessible to administrators.
- Segregate the networks: Separate corporate networks and systems from the ones managing customer data to prevent lateral movement from one to the other.

18. 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?

An important element of any ISMS (Information Security Management System) is vendor risk assessment. As part of this assessment, it's important for organisations to ask the right questions of their vendors and make a risk decision based on the nature of the information that this vendor will be processing/handling. In the case of Video Surveillance or Access Control systems, the impact could be very high for many organisations. It's important to ensure that any vendor meets or exceeds your own organisation's security controls and make the call on whether the risk is acceptable or not when they do not.

For example, you must ask questions such as:

- Is the vendor owned or part owned by a foreign government?
- Has the vendor or their products been banned, or are the in the process of being banned or restricted by other governments that are allies of Australia such as the United States of America or the United Kingdom?
- Does the vendor employ Multi Factor Authentication?
- Does the vendor perform regular penetration tests?
- Was the vendor victim of any breach? Were they transparent about the breach and act in good faith to quickly communicate and remediate the problems?
- Does the vendor have a Secure Software Development Process?
- Does the development, manufacture, or testing of the products breach ethical standards?
- Do products employ problematic algorithms designed to identify minorities and/or supress human rights?

There are many examples of these assessment questionnaires online that can be used as a baseline. More than just asking the questions, it's also important to ask for artefacts that support the answers to these questions, furthermore, asking for a third-party certification such as SOC (Service Organization Control) 2 Type 2 and ISO27001 will give assurances that these controls are properly implemented.

Lastly, it's critical to request audit rights so that the government can validate that data is being handled appropriately at any given time.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

Early physical security systems were based on analogue technology. The move from analogue to IP (digital) happened about 25 years ago. And now, this technology is moving to the cloud (and hybrid cloud).

Historically, physical security systems have lagged in terms of cyber security compared to other solutions coming out of the high-tech industry. But recent evolution, and the fact that the same information systems are used for physical security systems, the same cybersecurity best practices need to be embedded into these systems.

Ideally, the goal is to accelerate the adoption of cyber practices in the physical security field which may remain behind its IT peers. What is problematic is that some physical security manufacturers have focused on the basics to support a cybersecure image while they remain immature in the actual practice (for example: the hiring of strawman “CISO’s” or “CSO’s” is one common way companies work to camouflage a weak cybersecurity track record). This makes it difficult for users to distinguish between superficial cyber maturity efforts and vendors that have invested in deep cyber security initiatives and developing a mature practice as part of technology delivery. The government needs to build its own internal expertise to ensure appropriate choices are made.

In addition, since physical security systems have longer lifecycles than average IT systems, vulnerabilities will remain an issue for longer if not uncovered up front. IoT devices (IP cameras, controllers, etc.) that are part of the full system can introduce vulnerabilities if selected based on lower price rather than cyber maturity. This increases the need for greater cyber security awareness and guidance for procurement of physical security systems, their manufacturers and installers.

Finally, another issue the government should be aware of in this area is that there is a lack of tools to implement cybersecurity at scale. With so many IoT vendors, many different tools need to be used in deploying physical security. In addition, there are knowledge gaps with physical security integrators who are not IT and cybersecurity experts with limited experience with advanced cyber features (i.e. deploying X.509 certificates to using secure protocols such as HTTPS). Therefore, selecting the right integration partners is also critical to protect networks.

20. How should government measure its impact in uplifting national cyber resilience?

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?