# Response to 2023-2030 Australian Cyber Security Strategy Discussion Paper

Submitted by Veeam Pty Ltd

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

Building regional cyber resilience and improving the response to cyber incidents is a critical challenge that Australia and the region is striving to address.

Cyber threats are constantly evolving, making it clear that no single country can handle them alone. Collaboration between nations in the region is a priority to build cyber resilience and ensure a swift and effective response to cyber incidents. One way that this can be achieved is through enhanced information sharing, where threats are shared among countries. This can evolve into a common platform for intelligence sharing and incident reports, to allow regional cybersecurity agencies to stay updated.

Public-private partnerships can also come in to build the nation's cyber resilience. There could be more investment into training local talents, sharing information and challenges that industries face and finding solutions in a collaborative manner. Together, this can bolster Australia's relationship with its neighbouring countries and enhance our response to cyber incidents.

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

An effective automated threat-blocking model should involve three key components: standardisation, testing and secure backup. This will ensure a solid cybersecurity foundation for businesses as they grow and expand.

As businesses expand, standardised threat-blocking processes minimise time spent managing multiple systems, while also allowing teams to reduce time spent manually monitoring and blocking threats. Businesses can leverage specialised software such as threat intelligence platforms to detect and block threats quickly and efficiently, saving time and resources. When implementing vulnerability scanning and patching processes, businesses should use a risk-based approach, whereby vulnerabilities that have the most impact and/or are the most high risk are prioritised.

While automation can alleviate pressure and time spent on manual workloads, systems must be constantly tested for resiliency and effectiveness. This ensures that unauthorised access is effectively blocked and that any gaps in vulnerability management are addressed.

Finally, any cybersecurity model must include a robust disaster recovery strategy to ensure data can be efficiently restored in the case of an attack or breach. As no model is immune to cyberattacks, a disaster recovery plan is crucial to minimise business disruption and downtime. As businesses expand, this component will become increasingly important, as any cyberattack will impact more stakeholders. Veeam recommends following the 3-2-1-1-0 golden backup rule, where there are three copies of data (one primary and two backups) with two copies stored locally on two formats (network-attached storage, tape, or local drive), one copy stored offsite in the cloud or secure storage, and that all backups have zero errors after recoverability verification.

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

The government can look at supporting Australia's cyber security workforce through various initiatives. Increased investment in cybersecurity education and training programs, for example, can address the skills gap in the workforce. A national cybersecurity accreditation scheme can be implemented to establish a minimum standard of cybersecurity competency for professionals in the industry. This can help to ensure that those working in the field are qualified and competent, and can provide greater confidence to employers and customers.

Support in upskilling across non-IT professionals can also help alleviate pressure on cybersecurity professionals. The government must acknowledge that cybersecurity needs to be integrated into all roles across organisations. Further, there are merging of responsibilities across IT teams, though many do not have the capacity and opportunity to upskill. It is no longer the sole responsibility of IT teams to protect against cyber attacks, but rather, it is a collective responsibility.

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

An effective post-incident review and consequence management model with industry would involve several key components: rapid response, investigation, reporting, consequences management and a plan to improve.

This would entail a thorough start-to-end approach that addresses the issue, understands the causes behind it, and post-report before implementing the right legal or disciplinary actions and making the necessary changes to improve current practices. Having this standardised across the industry will ensure that organisations can identify vulnerabilities, respond quickly to incidents and minimise the impact of future incidents. This can help enhance overall resilience and stay prepared for the evolving cyber security threat landscape.

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

**a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?**

Cybersecurity strategies can be overwhelming to small businesses that have limited resources and knowledge on the subject matter. The government and industry can support these businesses by providing a centralised platform to disseminate information and resources. It is also crucial to emphasise that effective cybersecurity strategies do not need to be complex or require a large investment. If businesses can implement best practices for cyber hygiene, such as backing up data regularly, installing antivirus software, having a strong firewall, and ensuring that employees are well-versed in identifying suspicious links to avoid clicking on ransomware emails. This can deter and reduce the chances of a cyberattack, and make it easier for SMEs to recover if they are compromised.

The more SMEs buy into the need for good digital hygiene, the more alert they become. Safeguarding data along with regulating your cyber policies should be made mandatory. Cyberattacks are real, and measures to prevent them should not be neglected, irrespective of the scale of each business.