

AUSTRALIA'S NEW

# Cyber Security Strategy

 What does it mean for small  
and medium businesses?



**Veracity**  
Business Solutions



Late last year, the Australian government released its 2023–2030 Australian Cyber Security Strategy which outlines the Australian government's aim of making Australia a world leader in cybersecurity by 2030.

As part of the Strategy, cybersecurity will shift from being a technical topic reserved for those in the IT and technology sector to being a whole-of-nation endeavour to better protect individuals and businesses from cyber criminals and cyber attacks.

The Strategy comes after a year where millions of Optus and Medibank customers had their personal data leaked in high-profile cyber attacks.



# Cyber attacks are on the rise

Cyber criminals are becoming more sophisticated with their attacks, and cyber crime is on the rise.

In fact, the Australian Signals Directorate's 2022-23 Cyber Threat Report revealed that cybercrime reports were up 23 percent year-on-year, and a cyber crime is now reported every 6 minutes. Alarming, this is probably an underestimate when factoring in unreported cyber breaches.



**Veracity**  
Business Solutions



# Where are businesses most vulnerable?

Malicious cyber attacks often exploit unpatched and misconfigured systems or take advantage of weak or re-used credentials to access systems and networks. The Australian Cyber Security Centre warns that half of vulnerabilities are exploited within two weeks.

The top three cyber crimes reported by businesses:




- Email compromise.
- Business email compromise fraud.
- Online banking fraud.





# Cybercrime business costs increased by 14%

The self-reported costs of cybercrime for businesses:

-  Small business: \$46,000
-  Medium business: \$97,200
-  Large business: \$71,600





# So, what is the Cyber Security Strategy?

The 2023–2030 Australian Cyber Security Strategy aims to position Australia as a world leader in cyber security by 2030 through a three-phased horizon approach.





- **Horizon 1: Strengthen our foundations (2023–25)**  
By addressing critical gaps in Australia’s cyber shields, building better protections for our most vulnerable citizens and businesses, and supporting initial cyber maturity uplift.
- **Horizon 2: Expand our reach (2026–28)**  
By scaling cyber maturity across the whole economy and making further investments in the broader cyber ecosystem, continuing to scale up our cyber industry and growing a diverse cyber workforce.
- **Horizon 3: Lead the frontier (2029–30)**  
By advancing the global frontier of cyber security and leading the development of emerging cyber technologies adapt to new risks and opportunities across the cyber landscape.



## A focus on business

The Strategy has put a focus on businesses and promises to create a “ransomware playbook” to guide businesses on how to prepare for, protect against and respond to cyber attacks. The government will also explore how to make it easier for businesses to report cyber incidents through a single reporting portal.

As part of the \$586 million plan, the government has committed to better-protected infrastructure, while also funding cyber awareness programs to better educate individuals and businesses.







# Cyber security shields

The Strategy is a roadmap to help Australia become a world leader in cyber security and to better protect Australian businesses and individuals from cyber risks. To achieve this, Australia will implement six cyber shields in collaboration with the technology and IT industry with additional defences against cyber threats.

1. Strong businesses and citizens
2. Safe technology
3. World-class threat sharing and blocking
4. Protected critical infrastructure
5. Sovereign capabilities
6. Resilient region and global leadership





# What cyber security support will be available to businesses?

Australia's Cyber Security Strategy will mean that businesses need to prepare for a raft of new cyber obligations including cyber incident reporting and incident response frameworks.

However, there will be support available for businesses like cyber security awareness programs, advice and requirements for developing cyber security frameworks, access to grants and funding, and free cyber "health checks".





# Need a hand understanding the cyber security posture for your business?

Get in touch with Veracity and we can help you to assess vulnerabilities and provide support for developing Cyber Incident Response Plans (CIRP) and Cyber Incident Roles (CIR).

We can also assist you in designing and implementing your data governance framework to strengthen and test your cybersecurity controls.



# Get in touch!

 1300 850 172

 [hello@veracity.com.au](mailto:hello@veracity.com.au)



**Veracity**  
Business Solutions