mailguard

AT A GLANCE:

‘AUSTRALIA’S 2020 CYBER SECURITY STRATEGY’ - INDUSTRY ADVISORY PANEL REPORT

At a glance

‘Australia’s 2020 Cyber Security Strategy’ Industry Advisory Panel Report’ was released last week. Here's a quick summary of what you need to know:

- "*The 2020 Cyber Security Strategy Industry Advisory Panel was formed in November 2019 and asked to provide advice from an industry perspective on best practices in cyber security and related fields; emerging cyber security trends and threats; key strategic priorities for the 2020 Cyber Security Strategy; significant obstacles and barriers for the delivery of the 2020 Cyber Security Strategy; and the effect of proposed initiatives on different elements of the economy, both domestic and international.*"

The report provides important context for the state of our digital economy, the challenges that we face, and the leadership shown on cyber security by The Australian Government, with the development of Australia’s 2020 Cyber Security Strategy and the announcement of a $1.35 billion investment (Cyber Enhanced Situational Awareness and Response package) over the next 10 years.

“Our Government’s goal is for Australia to be a leading digital economy by 2030. Our degree of success will be critical to income growth and job creation over the next decade and beyond. Our extensive policy agenda encompasses digital access, connectivity, consumer data and competition policy, government service delivery and skills development, trade and global e-commerce governance, as well as the necessary focus on security and privacy concerns.”

- Prime Minister Scott Morrison (BCA annual dinner keynote 21 November 2019)

At a glance

The report states:

- "*The scope and timing of that ambition is well placed. As we enter the 2020s the world is on the exciting cusp of a fourth industrial revolution driven by connectivity and digital technologies... With so much at stake, robust and effective cyber security has never been more important and the 2020 Cyber Security Strategy Industry Advisory Panel welcomed the opportunity to contribute to that outcome*."

- "*The Panel were engaged in late 2019 at a time when the Federal Government were reviewing the progress of the landmark 2016 Cyber Security Strategy*."

It quotes Minister for Home Affairs, Peter Dutton, describing how meeting the evolving cyber challenge is key to Australia's economic prosperity and national security. In September 2019 he said:

- *"Cyber security has never been more important to Australia's economic prosperity and national security. In 2016, the Australian Government delivered its landmark Cyber Security Strategy, which invested $230 million to foster a safer internet for all Australians. Despite making strong progress against the goals set in 2016, the threat environment has changed significantly and we need to adapt our approach to improve the security of business and the community."*

- *"Cyber criminals are more abundant and better resourced, state actors have become more sophisticated and emboldened, and more of our economy is connecting online. Cyber security incidents have been estimated to cost Australian businesses up to $29 billion per year and cybercrime affected almost one in three Australian adults in 2018."*

"The Federal Government's top priority is protecting our nation's economy, national security and sovereignty. Malicious cyber activity undermines that."

- Prime Minister Scott Morrison (30 June 2020)

The Panel's recommendations are structured around a framework with five key pillars:

1. **Deterrence:** deterring malicious actors from targeting Australia.
2. **Prevention:** preventing people and sectors in Australia from being compromised online.
3. **Detection:** identifying and responding quickly to cyber security threats.
4. **Resilience:** minimising the impact of cyber security incidents.
5. **Investment:** investing in essential cyber security enablers.

Here's a summary of the panel's recommendations

1 Deterrence

*"On **deterrence**, we recommend that the Government establish clear consequences for those targeting Australia and people living in Australia. A key priority is increasing transparency on Government investigative activity with more frequent attribution and consequences applied where appropriate. Strengthening the Australian Cyber Security Centre's ability to disrupt cyber criminals by targeting the proceeds of cybercrime derived both domestically and internationally is a priority."*

2 Prevention

*"On **prevention**, the recommendations include the pursuit of initiatives that make businesses and citizens in Australia harder to compromise online. This includes a clear definition for critical infrastructure and systems of national significance with a view to capturing all essential services and functions in the public and private sectors; consistent, principles-based regulatory requirements to implement reasonable protection against cyber threats for owners and operators of critical infrastructure and systems of national significance; measures to build trust in technology markets through transparency such as product labelling; and the extension of existing legislative and regulatory frameworks relevant in the physical world to the online world.*

Ultimately cybercrime is just crime, cyber espionage is just espionage and hacktivism is just activism online. All levels of Government should take steps to better protect public sector networks from cyber security threats.

Government agencies should be required to achieve the same or higher levels of protection as privately-owned critical infrastructure operators. Different levels of government should collaborate to share best practices and lessons learned. Ultimately Governments should be exemplars of cyber security best practice and Australian governments have some way to go in achieving this aspiration."

Here's a summary of the panel's recommendations

3 Detection

*"On **detection**, recommendations include that Government establish automated, real-time and bi-directional threat sharing mechanisms between industry and Government, beginning with critical infrastructure sectors. Government should also empower industry to automatically block a greater proportion of known cyber security threats in real-time including initiatives such as 'cleaner pipes'."*

4 Resilience

*"On **resilience**, recommendations include the development of proactive mitigation strategies and strengthening of systems essential for end-to-end resilience. Government should strengthen the incident response and victim support options already in place. Speed is key when it comes to recovering from cyber incidents and Government should hold regular large scale and cross-sectoral cyber security incident response exercises to improve the readiness of interdependent critical infrastructure providers and government agencies.*

Resilience includes both the ability to recover from a cyber-attack as well as the redundancy designed-in to systems and processes. In other words, a key factor influencing the ability to recover is the level of redundancy present in systems in the first place. It is important to also call out that a number f recommendations to build resilience relate to the role of the individual, in particular around building cyber awareness. In this regard there is an important distinction between cyber security (which means protecting data and information networks and critical infrastructure functions) and cyber safety (which means protecting users from harmful online content).

The fundamental ability to participate safely online is the difference between enjoying the internet's abundant information resources and opportunities, and being a potential victim of a cybercrime."

Here's a summary of the panel's recommendations

5 *Investment*

*"On **investment**, recommendations support the ongoing development of highly specialised and effective capabilities exemplified by the Australian Cyber Security Centre and the state-based Joint Cyber Security Centres.*

This existing capability should be substantially increased and enhanced through significant investment and a more integrated governance structure that maintains an industry leadership role. It is going to be a critical enabler to the success of the 2020 Cyber Security Strategy.

The Panel is also of the view that it is important for Government and industry to continue to invest in cyber skills development and security risk management in Australia. Good enterprise security management includes all aspects of securing people, property and technology. This skills investment is recommended at both a professional and specialist skills level and also more broadly, and should include primary, secondary and tertiary courses (including programs that focus on all aspects of enterprise security risk management, particularly cyber skills uplift).

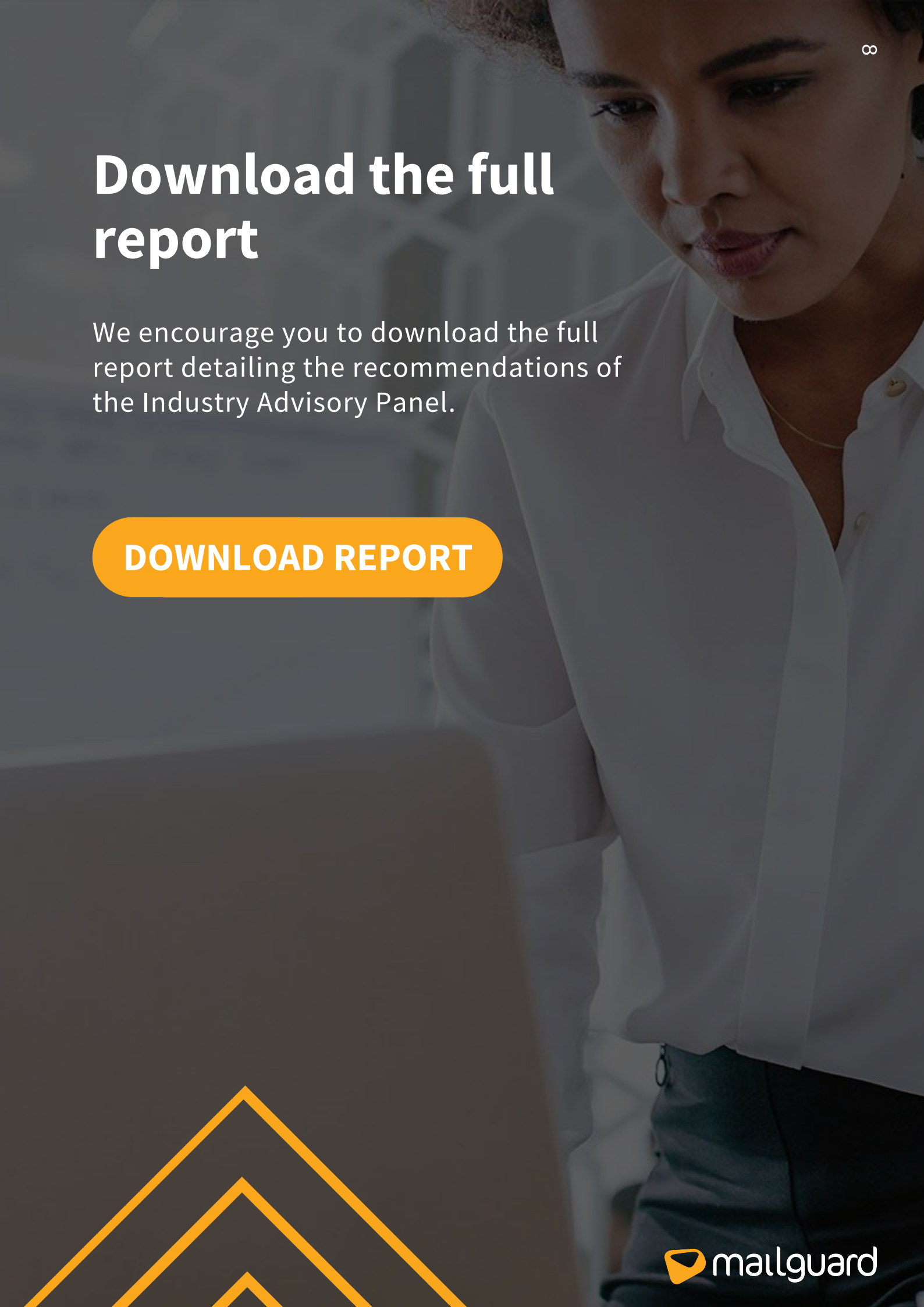
Importantly, many of these skills should be built as foundational requirements in science, maths, engineering and technology.

Although the cyber skills and awareness of directors on the boards of Australia's listed companies has been developed in recent years, there is opportunity for further development and support."

Download the full report

We encourage you to download the full report detailing the recommendations of the Industry Advisory Panel.

DOWNLOAD REPORT



mailguard

Email-based cyber-attacks are becoming more targeted, complex and pernicious.

If you don’t act, your business may be the next headline. To learn more about protecting your business against malicious email threats, like phishing, ransomware and BEC, reach out to the MailGuard team for a no-obligation chat.

GET IN CONTACT

mailguard