Since cybercrime impacts all Australians, how can Australia coordinate a collective response?

EY's submission to the development of the Cyber Security Strategy 2023-2030

Australian Government

15 April 2023

The better the question. The better the answer.
The better the world works.

Building a better working world

Building a better working world

Expert Advisory Board
2023-30 Australian Cyber Security Strategy
c/- Department of Home Affairs
Australian Government

15 April 2023

EY's view to Australia's 2023 Cyber Security Strategy

Dear Members

We enclose EY's submission to the 2023-2030 Australian Cyber Security Strategy – Discussion Paper, released in support of the Strategy's development, announced by the Minister for Cyber Security, the Hon Clare O'Neil MP, on 8 December 2022.

EY considers that Australia's next Cyber Security Strategy should be founded on three overarching principles:

1. **Citizen-centricity**, where the focus moves from penalising victims to protecting citizens and organisations, while better targeting malicious cyber actors.
2. **Collective defence**, with a shift in focus from reaction to prevention and response.
3. **Investment in cyber security capability** at a level commensurate with the cost of malicious cyber activity to Australia's economy and community.

We also urge the Expert Advisory Board to consider whether further, stand-alone cyber security legislation is required. Australia's many existing laws and regulations are not being fully applied to the digital domain. This should be the first line of enquiry, along with clarifying standards of practice within relevant existing regimes, ahead of adding further federal legislation.

Additional, stand-alone legislation risks further confusion around entity and individual obligations. It also risks degrading our sovereign ability to adapt to the near-term disruptive effects of step-changing technologies such as quantum computing, generative AI and outer space-based communications. Within the commercial context, it also risks decreasing supply and value chain competitiveness and Australia's ability to deliver against industry driven commitments under trade agreements, at a time when these economic and security factors have never been so important.

We would be pleased to discuss our submission with the Expert Advisory Board and look forward to doing so. We are also able to support you to engage with clients across our firm's service lines in Audit, Assurance, Strategy & Transactions and Consulting, in Australia and across our global network of over 700 locations.

Yours sincerely

[redacted]

Richard Bergman
Lead Partner, Oceania Cyber Security

[redacted]

Michelle Price
Partner, Oceania Cyber Security

Submission for Australia's 2023-30 Cyber Security Strategy

A balanced and sustained national approach to cyber security is critical for the wellbeing of every Australian public and private organisation and citizen – and the competitiveness of our nation. All the indicators suggest Australia is not where we need to be in our levels of cyber maturity, cyber resilience and integration of cyber security and privacy with standard economic practices.

The last few years have been characterised by the:

- **Increasing frequency and severity of cyber attacks.** Incidents of all kinds are increasing, with Australia continuing to be targeted by the full range of malicious cyber actors. The Australian Cyber Security Centre's most recent Annual Cyber Threat Report1 noted cybercrimes being reported every seven minutes. The ultimate victims of the vast majority of these attacks were Australian citizens.
- **Growing cost to the economy.** The University of New South Wales' Institute for Cyber Security estimates that cybercrime is costing Australia up to A$42 billion a year2.
- Ongoing lack of cyber maturity in our organisations. For example, the Commonwealth Cyber Security Posture in 2022 report3 found low maturity levels across agencies and departments in the Australian Government with low to moderate engagement with the Australian Signals Directorate's cyber defence services. There are increasing levels of technology debt and legacy systems, particularly within government, and yet we are not seeing a commensurate and proportional level of investment in cyber capability.

To deliver on the Minister's aspiration for Australia to become the world's most cyber secure nation by 2030, we must do more than simply refresh our national cyber security strategy. A fundamental strategy reset, a refocus on citizen centricity and incident prevention and significant, considered and long-term investment are required to make a step-change in our ability to counter cyber threats.

Note: EY is responding to selected questions from the Discussion Paper and we have used the order of the questions as they appear in the document accordingly.

[1] ACSC Annual Cyber Threat Report, July 2021 to June 2022, November 2022, Australian Government. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

[2] Cybercrime in Australia: 20 years of in-action, Nigel Phair, November 2021. UNSW Press.

[3] The Commonwealth Cyber Security Posture in 2022, December 2022, Australian Government. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/commonwealth-cyber-security-posture-2022

EY Response to National Cyber Security Strategy

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?

We recommend the National Cyber Security Strategy is founded on three overarching principles: citizen-centricity, collective defence and commensurate investment.

Citizen-centric approach

To protect the citizens whose lives and jobs are being disrupted by cybercriminals, we must design penalties to punish aggressors – not victims. This will require **harnessing behavioural economics to find drivers that produce the outcomes we want,** that: citizens are protected; companies are incentivised to invest in cyber security proportionate to their upside and downside risk landscape and only punished for genuine malpractice; and malicious actors are stopped, and where possible, caught and penalised.

The current discussion paper does not appear to be focusing on this premise. For example, it foreshadows the Government making paying ransoms illegal. While this is the time-honoured response to kinetic matters such as kidnapping, it does not make sense in the nuanced and complex cyber world. **Prohibiting ransom payments would ultimately benefit cybercriminals by adding to the destruction they cause** while creating complex and possibly morally challenging dilemmas for companies, who will be caught between conflicting regulations, and poor outcomes for citizens.

Attacks on cyber-physical systems are increasingly likely to result in fatalities[4]. Organisations have both a fiduciary responsibility and a moral imperative to save lives. Fining organisations for doing the right thing – whether saving a life, protecting citizen data and/ or making informed choices for which conflicting domestic and/or international regulations they will breach – just adds to the damage caused by malicious actors.

We note that some jurisdictions internationally attempting to introduce such reforms have endured unintended consequences, in particular where a reasonable level of overarching cyber maturity across sectors is not in place.

Organisations, including government bodies and non-profits, demonstrating systemic cyber under-performance should be held to account. But we must **consider that context is paramount against what constitutes the "right cyber setting".** Where does an entity sit in relation cyber maturity in its industry? What level of investment is available to uplift its cyber risk management? If a critical infrastructure owner depends on regulators to approve funding for cyber security, will we fine that entity if is not afforded sufficient funds to defend its critical assets?

If we use the blunt instrument of blanket legislation, aggressive penalties could also send small businesses bankrupt. Small businesses make up 97% of the economy and employ more than five million people[5]. Putting them out of business for being under-prepared for a cyber attack will further undermine Australia's economic wellbeing.

A more practical approach would only see penalties levied where decision making, controls and processes are below baseline standards for the industry and organisation size (see *Collective defence* section (next page)).

[4] Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans, July 2021, Gartner. https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

[5] Contribution to Australian Employment, August 2022. Australian Small Business and Family Enterprise Ombudsman. https://www.asbfeo.gov.au/sites/default/files/2022-08/Contribution%20to%20Australian%20Employment_August%202022.pdf

EY Response to National Cyber Security Strategy

Finally, if Commonwealth departments and agencies are to serve as a model for other entities, they must **solve the trust deficit with citizens.** According to a 2020 report by the Department of the Prime Minister and Cabinet, "only three in ten Australians trust government services, well below levels for leading governments and private-sector businesses".[6]

New EY research[7] also found that, despite the widespread use of digital government services and general positivity about them, many Australians remain concerned about privacy and potential data breaches. For example, single digital IDs could be a critical enabler of digital government services and reduce the risks of identity fraud. But almost three in ten Australians are still uncomfortable with the concept. To address this issue, Government will need to embed security mechanisms from the outset, start with a voluntary system (akin to the My Health Record rollout) and establish an independent governance authority to build public trust.

Collective defence

To create a sovereign and assured capability to counter cyber threats, we must shift from our reactive stance and focus on collective prevention. The discussion paper acknowledges this but is silent on how Government will support this kind of collective defence mentality.

As a starting point, we recommend investing in Australia's sovereign cyber capability above and beyond our current ambitions. We suggest targeting a capability that takes a hybrid of the US **Information Sharing and Analysis Centres,** which handle threats in sector context and risk translation against maturity, and Israel's national **Cyber Emergency Response Team** (CERT), which handles cyber incidents in the civilian cyber sphere and has visibility of risk across critical infrastructure and five sub-centres dedicated to specific industries, all operating under the same roof.

We also need better and sustained **public private partnerships**, with big tech, government, industry and academia working together both on forming collective defence at a national level and developing an advanced sovereign cyber capability across emerging technologies.

Australian industry and academia are highly credible on the global cyber stage. We should give them a bigger and more explicit role in our collective defence, also positively impacting the management of systemic risk in supply chains.

Building a collective defence depends on transparency, consistency and cohesion. In the more than a century-old practice of law, we have intense transparency as to what bad, good and great looks like.

In contrast, the immaturity of Australia's cyber posture means we lack transparency around how Australia's collective cyber infrastructure functions should be measured and how it is impacted by externalities like the law. We are also currently operating with many inconsistencies across layers of government and between and within industries.

We need a cohesive and collaborative approach, focused on prevention – one that clarifies the current tangle of cyber laws, regulations and expectations. An exemplar is the UK's National Cyber Security Centre, which takes a supportive and collaborative approach to improving cyber protection, including:

- Responding to cyber incidents to reduce the harm they cause to organisations and the country.
- Using industry and academic expertise to nurture the UK's cyber security capability.
- Distilling national knowledge of cyber security into practical guidance.

To set entities up for success (and support transparency and outcomes measurement), we must **set appropriate baseline standards** within existing regimes for different entities – critical infrastructure, large companies, small organisations, central government departments and all other government agencies – and potentially different types of data (e.g., health data is particularly sensitive). A starting point for this is work undertaken in partnership between the NSW Government and industry on baselining cyber security standards and practices, providing a framework to accelerate a whole of economy equivalent.[8]

As part of this, the efforts by the Government and collectives in industry to tackle cyber threat sharing, and separately the larger challenge of information sharing requires an evolved approach if we are to truly embed cyber security practices in the economy and social norms of behaviour.

A national framework of common technical methodologies, enhanced with the ability to adapt to the technological changes posed by artificial intelligence and quantum, is now required. This is fundamental to the success of the Strategy's 2030 aspiration as well as other major Government endeavours such as the AUKUS security pact and delivery of the National Reconstruction Fund. The framework should also transparently take account of existing and emerging regulatory regimes on data management such as the Notifiable Data Breach scheme and the Consumer Data Right.

We also need to create a **comprehensive incentives structure** to support organisations to understand and meet these baseline standards. Other countries have discovered the collective benefits of a collaborative cyber defence response via large-scale communities of interest.

---

[6] Our public service our future,201. Department of the Prime Minister and Cabinet. https://www.pmc.gov.au/sites/default/files/resource/download/independent-review-aps.pdf

[7] Connected Citizen, 2023. EY

[8] Recommendations Report of the NSW Cyber Security Standards Harmonisation Taskforce, February 2021. NSW Government. https://www.nsw.gov.au/news/release-of-cyber-standards-recommendation-report

EY Response to National Cyber Security Strategy

For example, US counties are working through risk management, legals and cyber insurance collectively. Australian small business associations could do the same. To support this, we will need contextualised use cases and case studies so organisations can see the benefit of coming under a collective cyber defence umbrella.

We must also put in place **transparent and lawful countermeasures for active defence** such as those described under MITRE Engage[9], and ensure appropriate provisions for ethical hackers to protect their work as part of our sovereign capability. Ethical hackers are currently underutilised elements of collective defence. We must offer them an appropriate safe harbour if we are to successfully anticipate the actions of, identify and defend against increasingly sophisticated attackers.

Commensurate investment

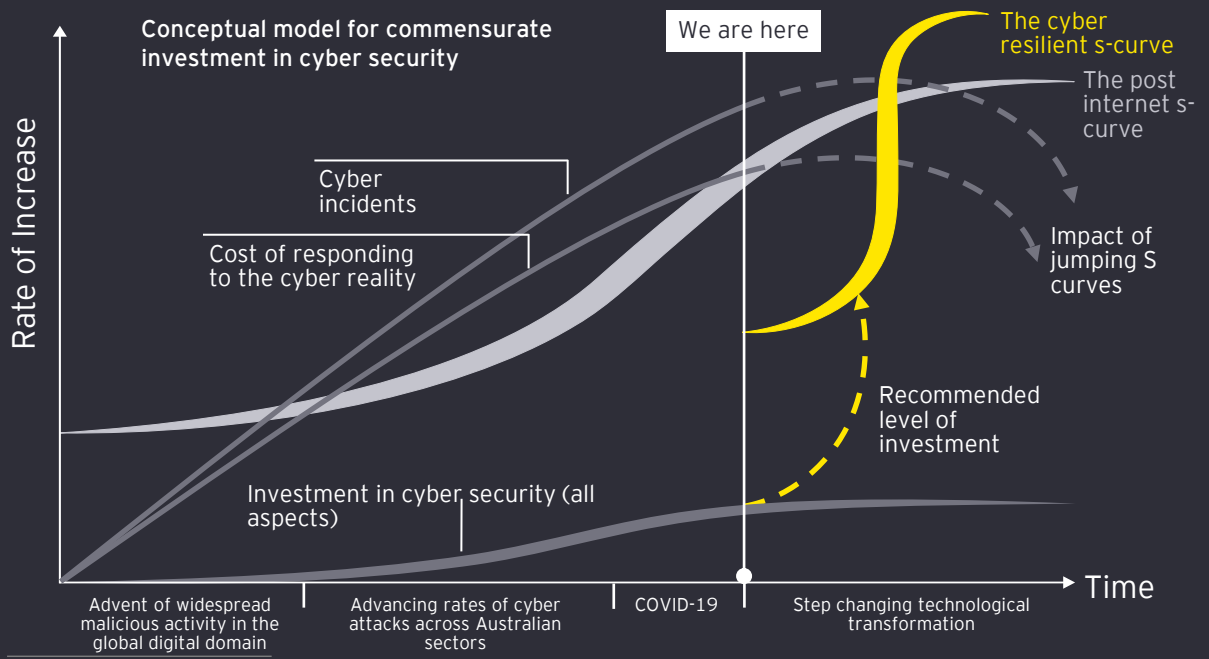
Government and industry need to invest appropriately to protect citizens' data and their right to privacy, and to defend our critical infrastructure.

The limited data coming from government and vendor sources does not paint a coherent story of what is happening in cyber security. We must understand how much all forms of **malicious cyber activity are costing our economy in totality and within demographic and sectoral constructs**. Because cyber security and privacy as an industry is fledgling, there is limited independent and robust Australian data on the critical elements of cyber incidents, their cost, or the level of investment in cyber defences.

We strongly encourage the Government, in partnership with relevant sophisticated industry and academic sources, to develop appropriate productivity-driven methodologies to measure and consistently document the above critical elements. It should then compile baseline data and provide transparent benchmarking to enable future-back planning for all organisations and collectives at a sectoral level, including informing the Government's own ongoing investment in cyber security.

Using the appropriate data from this effort, we recommend investing 10% of the annual cost of cybercrime each year (around A$4 billion per year) as a starting point. Around half of this investment should go towards hardening Australia's organisational cyber capabilities and growing Australia's cyber security industry in its capacity and maturity. The other half should be put into a sovereign cyber investment fund to accelerate buildout of sovereign defence capabilities through collaboration between government, industry and academia, leveraging in part a 'secure by design' approach to all sovereign investments made through the Government's National Reconstruction Fund.

The Government should also look to provide long-term funding to its agencies to uplift their cyber security and workforce capacity, and look to share knowledge where possible with State, Territory and local governments. The current practice of providing short-term, project-based funding streams has created significant legacy security risk across government ICT with the build and renewal effort now at crisis point. This is of disproportionate concern for Australia, in a large part because of the structural dominance of its public sectors. The impacts of commensurate investment would serve to drive down the volume and severity of incidents impacting Australia, together with their cost, while also driving up cyber maturity and resilience. This is demonstrated conceptually overpage leveraging the S-Curve approach.



[9] MITRE Engage™ | An Adversary Engagement Framework from MITRE https://engage.mitre.org/

Enhancing and harmonising regulatory frameworks

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

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

Yes. The *Corporations Act 2001* should be amended to specifically address cyber security risks and consequences, as well as make commensurate adjustments for privacy per reform underway in that aspect of law. Otherwise, directors will be inadvertently incentivised to overlook cyber security to drive profitability. We need to shift majority current behaviour, where organisations generally deal with security risks comprehensively when they become an urgent issue. Cyber transformation and risk management should be driven from the top. Directors need clear signals that they are expected to invest ongoing in protecting citizen data and, where relevant, infrastructure against cyber attack.

D Should Australia consider a Cyber Security Act, and what should this include?

No. Cyber security should be explicit, rather than implied, in the legal frameworks of existing corporate and critical infrastructure requirements. The Government should place emphasis on supporting organisations of all sizes to meet existing requirements, make this explicit, and also allow time for the newer security obligations and mandates to take full effect.

An additional Act would likely lead to over-regulation and increase the burden and complexity of compliance. At a time when the nation is recognising the security and privacy implications of the over-collection and over-sharing of data along with the unnecessary storing of sensitive information. It is also hard to see how such new legislation would become operational quickly. Creating a standalone Cyber Security Act will require a significant body of work and consultation, requiring harmonisation with multiple existing regulations, including, for example at the federal level, the *Telecommunications Act 1997*, *Telecommunications (Interception and Access) Act 1979, Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, Security of Critical Infrastructure Act 2018, Privacy Act 1988* and the Criminal Code. Industry and public sector organisations need guidance now around what baseline standards are expected, support to achieve them and incentives to collaborate in this task.

E How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

The Australian Government's Office of Impact Analysis could be expanded to help policy makers understand the impact of the regulatory burden on organisations. This could assist the Office with its core function of developing the evidence base for decision making. Security regulators at all levels of government could also be required to report on the regulatory burden of cyber security obligations in their annual reports to support transparency and longitudinal analysis of whether regulatory interventions are sufficient. As noted in other sections of this submission, the nation should better leverage existing regulatory frameworks and regimes to address cyber risk. In doing so deliberatively, this also gives rise to opportunities to streamline these frameworks, an ongoing requirement as malicious techniques continue to evolve and technological change continues to increase.

F Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

No. (a) Prohibiting ransom payments would ultimately benefit cybercriminals by adding to the destruction they cause, including creating poor outcomes for citizens and complex and possibly morally challenging dilemmas for organisations, who will be caught between conflicting regulations.
(b) Such a policy would be counter to international cyber insurance trends, which include clauses for customers to claim in a situation where a ransom is paid for legitimate reasons, such as saving a life. Prohibiting ransom payments will also create contradictions and complications in broader aspects such as business continuity insurance, workplace health and safety insurance and directors' insurance.

F.1 What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies, and insurers?

It would likely prevent directors from executing their fiduciary responsibilities, prevent organisations from protecting their employees and customers, and create conflicts with other regulations and insurance contracts. Existing common law treatment of cyber incidents should be tested as there are likely examples in this space that would highlight other unintended legal and moral conflicts.

Strengthening Australia's international strategy on cyber security

3

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

We can expand our efforts to help our neighbours develop their cyber security skills and maturity. In a turbulent geo-political environment, Australia has an increasing responsibility to ensure our allies in the Indo-Pacific have strong baseline cybersecurity capabilities to deter malicious actors. This is especially true for the Pacific Islands.

Australia's current program, the *Pacific Cyber Security Operational Network (PaCSON),* enables a select group of Pacific neighbours, including New Zealand, to cooperate and empower members to share cyber security threat information, tools, techniques and ideas between member nations.

However, Australia could be a stronger player in the region. For example, we could:

- Spearhead the creation of an Indo-Pacific Hybrid Threat Centre, mirroring the NATO-EU Hybrid Centre of Excellence. This entity could potentially work in collaboration with Singapore's ASEAN-based ADMM Cybersecurity and Information Centre of Excellence.
- Rotate people through specific cyber roles with our neighbours to enable better collaboration, upskilling and knowledge transfer.

4

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

Australia should focus on supporting, and where appropriate scaling, existing mechanisms (e.g., APCERT, FIRST, PaCSON) rather than creating new ones, which will most likely result in duplication.

Cyber transformation and risk management needs to be driven from the top, which means Australia should be identifying opportunities to engage leaders, particularly in the Pacific Island Forum, to articulate the importance of prioritising cyber resilience.

Strengthening Australia's international strategy on cyber security

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?

The Australian Government is undertaking important global advocacy as a member of the International Telecommunications Union and as part of the United Nation's Open Ended Working Group in our contribution to the Group of International Experts. However, the bulk of our engagement has been within Asia-Pacific.

Australia must find more ways to expand its sphere of influence beyond Asia-Pacific, including engaging meaningfully with the powerful African bloc. Actions to consider include:

- Continuing to support strengthening engagement of Asia-Pacific delegates with the aim of ensuring they attend critical decision-making discussions. The OEWG Women in Cyber Fellowships and international law in cyber space training are practice examples of how Australia can boost engagement.
- Deploy specialist cyber staff to engage in key institutions and with regional bodies. Locations might include New York, Vienna, Geneva, New York, Ethiopia, Indonesia and Fiji.
- Create a value proposition for industry participation in relevant standard setting processes. This might include funding participation (similar to the model for International Labour Organization participation), enhancing access to senior officials.

Securing government systems

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

Departments and agencies across the Commonwealth are suffering significant technology debt and legacy due to short-term funding and policy strategies, mixed technology solutions and strategies that change constantly at short notice. These issues are hampering efforts to uplift cyber security capabilities.

To make the major step change required in cyber across departments and agencies, the Government should:

- Select one strategy to harden government IT and stick with it for longer than five years to allow sufficient time for initiatives to be implemented, fine-tuned and effective.
- Replace legacy systems that have reached end of life.
- Simplify enterprise architectures and remove duplication of systems.
- Establish whole of government cyber shared services to pool capability and drive consistency.

It is also important to remove blockers to enabling agile security projects within government. Attackers will not wait 12 months for a business case and funding to be approved or another 2-3 years for capability to be delivered to address current vulnerabilities.

8 During a cyber incident, would an explicit obligation of 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.

Yes. Separating the incident reporting to ACSC and compliance reporting (CISC) requirements will greatly improve collaboration between the Government and industry. Industry is already confused as to who they should and should not report to when they are experiencing an incident. Even with an explicit obligation of confidentiality, hesitancy to share information with government will remain an issue.

An independently funded body, which is legislatively protected from having to share information with Government, could be a more effective mechanism.

It was premature to put the Government Assistance Measures (GAMS) in SOCI, especially as the government is yet to publish the security and resilience rules to the Enhanced Cyber Security Obligations. The GAMs should be removed until the rest of the regulatory regime is more mature and we can see that a security baseline is increasing.

Securing government systems

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?

If the mechanism was industry-led, and complementary or appended to the Notifiable Data Breaches scheme, this could be beneficial.

Investment should be made in better communication and community awareness of the resources that are already available, and cyber security guidelines for consumers on how individuals can support our collective defence.

11 Supporting Australia's cyber security workforce and skills pipeline

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

The Strategy should identify the many skills and workforce development initiatives already underway across federal and state/territory funding and call for scaling those initiatives that will have the greatest generational impacts across demographic factors. Cyber apprenticeships and career changing pathways will be important to help generate the skilled workforce required to uplift national cyber capabilities.

The Government should also leverage the release of the Strategy to announce the preschool to Year 12 cyber security competency packages for the STEM curriculum developed under the national Digital Technologies Curriculum review completed at the end of 2021.

These packages were co-designed by the Australian Curriculum, Assessment and Reporting Authority and industry and should be complemented by a 'train the teacher' program (as submitted to the Department of Industry, Science and Resources in early 2022) to ensure consistent implementation and measurable advancement of skills development as children progress from year to year.

13 National frameworks to respond to major cyber incidents

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

Australia should focus on supporting, and where appropriate scaling, existing mechanisms (e.g., APCERT, FIRST, PaCSON) rather than creating new ones, which will most likely result in duplication.

Cyber transformation and risk management needs to be driven from the top, which means Australia should be identifying opportunities to engage leaders, particularly in the Pacific Island Forum, to articulate the importance of prioritising cyber resilience.

Designing and sustaining security in new technologies

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

Within the strategy's seven-year lifespan, the digital environment will be radically disrupted by emerging technologies, such as quantum computing, generative AI and outer space-based communication. Prescriptive, rigid, technical regulation will not keep pace with the coming changes.

Rather than being re-written, strategy must create room for baseline standards to be augmented and organisations to change their approach to cyber based on the impact of emerging technologies. As described above, the Government, in partnership with industry, should fund ongoing research into security risks and defences associated with emerging technologies.

Implementation governance and ongoing evaluation

20

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

By publishing national cyber maturity information similar to the way ACSC does for the Commonwealth Government. This will help organisations assess whether they are keeping up with peers, ahead of the curve or falling behind. It is essential to track and report on maturity uplift across the public and private sectors to assess the impact Government is having on improving overall national cyber resilience.

21

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

Additional to question 1, a publicly released balanced scorecard to measure implementation of initiatives within the strategy. This might include:

- The cost to implement policies versus the cost of remediating previous intrusions.
- Levels of consumer cybersecurity knowledge and overall cybersecurity confidence.
- Levels of compliance with baseline standards by organisational type and industry.

Eventually, the scorecard measures could expand to include:

- Cybersecurity ratings on consumer and Programmable Logic Controllers products to raise awareness and educate within the community while forcing manufacturers to consider cybersecurity.
- A de-identified list of potential intrusions mitigated by the Commonwealth and businesses, on a lagging 12-month basis, to support public transparency and raise awareness of the prevalent threats without creating alarm.

Contacts

Richard Bergman
Lead Partner, Oceania Cyber Security, EY
[redacted]

Michelle Price
Partner, Cyber security, EY
[redacted]

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

PH20233-002102
ED None

ey.com