CyberCX

CYBERCX CYBER SECURITY STRATEGY SUBMISSION

APRIL 2023

Contents

Foreword

CyberCX supports the government's ambition to make Australia the world's most cyber secure nation by 2030. To achieve this end state will require bold action.

Being a world leader in managing 21st century security risk is not new for Australia. We led the world in risk-managing the roll-out of 5G. We broke ground with our critical infrastructure reforms, regulation of online news and e-safety innovations. We were among the first countries in the world to appoint a cyber ambassador.

But despite these landmark moves, much of Australia's response to the ever-worsening cyber threat landscape has remained reactive and incremental. The 2023-2030 Cyber Strategy offers the opportunity for a reset.

As Australia's largest cyber security provider, CyberCX was founded with the mission to secure the communities our teams live and work in. Our submission reflects the significant operational experience of our people, who work every day to prevent, respond to and recover from cyber attacks against Australian organisations.

It presents realistic, high-impact measures that we consider will achieve value for money for the taxpayer.

Alastair MacGibbon
Chief Strategy Officer
CyberCX

Introduction

Australia's cyber threat environment is more complex and contested than at any previous time, and it is highly likely to deteriorate over the lifespan of this strategy.

Cyber criminals harm Australians and our organisations with near impunity and their business models are highly resilient and adaptive. Nation states have been emboldened by more than a decade of Russian cyber aggression and China's relentless information theft. As the Indo-Pacific becomes more volatile and authoritarianism resurges globally, the risks of cyber-enabled surveillance, disinformation and infrastructure disruption are growing.

These are not just "online" harms – cyber insecurity poses an existential threat to Australians' livelihoods and safety and to our economy, national security and democracy.

In this context, CyberCX welcomes the opportunity to make a submission to the 2023-2030 Cyber Strategy Expert Advisory Board. Our recommendations reflect three overarching philosophies:

1. **Managing cyber risk is a whole-of-nation responsibility.** Governments should lead initiatives only where industry cannot.

2. **Value for money.** As cyber threats worsen and digitalisation increases, the government will need initiatives that are effective and affordable.

3. **Outcomes matter.** All initiatives must produce outcomes that can be measured to ensure accountability and success.

Our submission advances five priorities, each with sub-recommendations:

1. **Improve Australia's response and resilience to cyber incidents**, making clear where the federal government leads and where the market must step up.

2. **Protect Australians from crime**, by substantially increasing the capability and attention of law enforcement agencies on cyber crime.

3. **Focus the market on improving Australians' cyber security,** by enhancing incentives and accountability structures and modernising regulation.

4. **End the cyber workforce shortage for the cyber century,** by backing sovereign capability and investing in a diverse workforce, supplemented by targeted skilled migration.

5. **Elevate Australia's international cyber security leadership,** focusing on our near neighbours and initiatives with likeminded partners.

1. Improve Australia's response and resilience to cyber incidents

Overview

The recent series of high-profile cyber incidents were entirely foreseeable yet caught Australia off guard. Data breaches are not the only cyber incident type that is foreseeable. So far Australia has been lucky to avoid cyber incidents with significant, cascading impacts on the availability or integrity of essential services and critical infrastructure. Our luck is unlikely to hold.

The federal government should clarify its roles and responsibilities, support and regulate private sector incident response and invest where the market will not – in the security of government itself and our democratic institutions.

Create a government 'front door' to streamline incident response

The problem

Major cyber incidents impact multiple sectors and stakeholder groups at the same time. Effective response requires mobilisation of expertise and resources from across government and industry and timely, multi-level crisis communications.

Currently, there is confusion over the roles and responsibilities of federal departments and agencies (including ASD, ACSC, the AFP and Home Affairs), regulators such as APRA and OAIC, state government cyber and portfolio departments, and ministers during a cyber incident. Victim organisations must engage with dozens of government stakeholders with often competing priorities, legislative footings and timelines for notification. Uncertainty and complexity make effective decision-making during an incident difficult. It can slow down victim access to government support and information. It can hinder important remediation actions (such as cancelling and reissuing compromised identity documents or notifying banks of potential fraud).

Additionally, effective crisis coordination can minimise harm caused by cyber incidents – for example by mitigating the social cohesion impacts of incidents that disrupt essential services or explaining to data breach victims the actions they can take. Currently, stakeholders receive conflicting communications – shareholder disclosures, customer emails, statements from bureaucrats and Ministers. There's no clearly authorised spokesperson to lead and streamline this process.

Solutions

Immediate term (2023)

- **The reconstituted office of the Cyber Security Coordinator (CSC) should be a victim organisation's government 'case manager', facilitating support from—and deconflicting priorities among—government stakeholders.** The CSC should be appropriately resourced and authorised to be a victim organisation's 'front door' to government during a major cyber incident. The CSC should lead information-sharing and mobilise government resources to support victims and other impacted stakeholders. Importantly, the CSC should not – or create expectations that the bureaucracy can – deliver incident response.

- **The CSC should provide a seamless notification portal for victim organisations.** Victims should only need to "notify once", with CSC cascading notifications across all other regulators and departments.

Short term (2024)

- **The CSC should release public guidance to clarify the roles and responsibilities of various government agencies during a major incident,** taking into account any relevant recommendations of the as-yet unreleased Mrdak Review.

- **The CSC should lead the government's law reform agenda to deconflict competing priorities in legislation and regulation.** One option is harmonising cyber security related laws into a single Cyber Security Act, but clarity could also be achieved through better policy guidance and law reform.

- **The CSC should develop and publish a National Incident Response Protocol.** This should include a framework for declaring a major national cyber incident and lexicon for assessing the criticality of incidents. Akin to a bushfire warning scale, likely incident impact can range from MODERATE to HIGH to EXTERME to CATSTROPHIC, depending on the nature and volume of any data stolen, which systems have been impacted and how, the follow-on impacts to the economy and society more broadly, and remediation options available. The Protocol should also cover crisis communications considerations, such as guidance to the Press Council of Australia on responsible reporting of major cyber incidents.

Longer term (2025+)

- **The government should consider expanding the CSC into an independent statutory body with a wider remit for all cyber security policy, with commensurate authorities and resources.** This would combine functions currently housed within the CISC, Home Affairs and ACSC and appropriately reflect the significance of the cyber security challenge to Australia.

Outcomes

- A government front door for incident response coordination
- Industry and public certainty about roles and responsibilities during cyber incidents
- Streamlined, faster support for victims and a need to only "notify once"
- A mature national approach to triaging and communicating about cyber incidents

Create a national marketplace for incident responders

The problem

ASD/ACSC has a world-leading reputation for computer security, including response investigations. But most of Australia's incident response capability exists outside of government, across ASX100, critical infrastructure entities and cyber security companies. In a national cyber crisis, it would largely be these workers keeping Australians safe.

Currently, there are market inefficiencies in how victim organisations connect with incident responders. Often, this is a decision driven by insurances or lawyers. Many victim organisations lack the information to assess incident responder quality and suitability.

Finally, cyber incident response is a national imperative, but it's not yet a regulated profession. Just as we saw with failures in the financial advice sector following the Global Financial Crisis, unregulated professions can result in harm to Australians.

Solutions

Short term (2024)

- **The government should build a national register of certified incident responders.** This will require government to first define incident response services and create a framework to identify and register incident response experts and organisations. This will also position government to create a feedback loop with registered providers, facilitating information-sharing and faster response activities.

Longer term (2025+)

- **The government should establish an industry working group to consider future industry standards and training requirements**, with a view to professionalising Australia's incident response industry.

Outcomes

- An efficient market for matching victim organisations with incident response experts.
- A trusted, highly capable Australian incident response profession.

Protect our democratic institutions from foreseeable cyber threats

The problem

Australia is not prepared for cyber attacks or cyber-enabled interference against our democratic institutions. Australia's non-profits, political parties and media organisations are victimised by both cyber criminal and nation-state actors, but often lack the resources and information to build cyber resilience.

Our critical democratic infrastructure includes civil society entities, the media, as well as public bodies including electoral commissions, courts and tribunals, parliaments and national institutions such as the National Archives.

Solutions

Immediate term (2023)

- **The government should publicly signal the criticality – and cyber vulnerability – of democratic institutions, and release targeted cyber uplift guidance.** For non-government organisations, this could be achieved by expanding the Security of Critical Infrastructure Act. For public organisations, an equivalent measure should be considered.

- **The government should commit to provide additional, targeted funding for democratic institutions' cyber resilience**. For non-government organisations, this could be achieved by expanding existing cyber and foreign interference support programs.

Short term (2024)

- **The government should establish accountability frameworks for democratic institutions to spur action.** For government organisations, accountability measures should be public and regularly reported on. Non-government entities could report to the CISC or an equivalent government agency.

Outcomes

- Awareness and access to information for all democratic institutions about the cyber threats they face.
- Government funding and other support to uplift democratic institutions' cyber resilience.
- Accountability frameworks to drive cyber security across our democratic institutions.

Invest in federal government cyber resilience by continuing the Cyber Hubs program

The problem

Funding for the Cyber Hubs pilot will soon expire. Continuing this programme is key to raising the baseline cyber security capability of our departments and agencies, improving coordination of investment and operational activities, and consolidating Australia's critical cyber workforce. While recent data breaches in the private sector have shocked the nation, a data breach of similar scale, especially of a citizen-facing department or agency, could have much more significant national impact. Government also has a primary duty to protect government services from being disrupted or degraded by criminal or nation-state activity.

Cyber Hubs lets government benefit from the efficiencies of scale. Government can't afford to silo capability in different departments and agencies – especially given budgetary pressures. Shared information and shared services are the pathway to better detection, response and resilience.

Solutions

Immediate term (2023)

- **Provide funding certainty by establishing Cyber Hubs as a permanent programme.**

Short term (2024)

- **Expand Cyber Hubs to service more departments and agencies**.

Outcomes

- Government fulfils its primary duty to provide government services and protect citizen data.
- Government receives value for money via the efficiencies of scale rather than developing inefficient, siloed capability.

2. Protect Australians from crime

Overview

Cyber crime is Australia's fastest growing crime type and impacts the most Australians, but law enforcement attention, investment and capability has not kept pace. Countering cyber crime is primarily a federal government responsibility as the criminals operate from outside Australia.

A dominant law enforcement focus of pursuing and prosecuting cyber criminals fails to acknowledge the scale and volume of 21st century cyber crime and the reality that it mostly comes from offshore havens. The most effective way for the Australian government to materially drive down cyber crime is to disrupt cyber criminal operations *before* they cause harm.

Conversely, we believe that banning ransom payments – at least in the short to medium term – will not materially reduce the frequency or harm caused by cyber crime in Australia. CyberCX does not encourage paying criminals. But without material uplift in law enforcement activity, a ransom ban would deprive organisations of a last resort measure to prevent catastrophic outcomes, such as harm to people, sustained disruption of essential services or loss of a business. Cyber criminals are also resilient and adaptive. Unless we significantly disrupt their businesses, criminals will reroute their operations around a ransom ban. This could include, for example, pressuring multinational companies to exploit loopholes in Australian laws, increasing targeting of small and medium enterprises to evade government thresholds, evolving tradecraft to increase harm so ransoms are still paid, or "forum shopping" by increasing targeting across our more poorly defended regional neighbours.

Task AFP to prioritise cyber crime, using its existing powers and networks to drive cost into offshore cyber crime operations

The problem

To protect Australians the AFP must proactively disrupt cyber criminal operations *before* they result in harm. The AFP's recent involvement in shutting down the cybercriminal forum Genesis Market was very welcome, but these type of multinational operations can take years to execute and occur too infrequent to materially affect the global cyber crime ecosystem.

The AFP already has authorities and oversight to disrupt cyber criminals in cyberspace, enhanced by the bipartisan *SLAID Act* 2021. In the short term, the AFP will need to partner with industry to generate the capability and skills for this mission, not that it will require exquisite cyber weapons. This mission can be achieved quickly and cost-effectively with widely available commercial tools.

Most useful of all is the AFP's established international liaison officer network, which was built over decades to tackle complex transnational crimes. This network will provide the mechanism for coordinating counter-cyber crime activities with global peers, including in cybercrime safe haven/source countries. Cyber crime needs to be made a priority, just as terrorism and organised crime have been in the past.

Over the longer term, the government needs to ensure AFP has the legislative footing and capabilities it needs to adapt to new cyber criminal threats and changing technology. Over the lifespan of the Strategy, Australia's law enforcement and intelligence agencies risk becoming reliant on support from the Australian Signals Directorate (ASD) to undertake cyber technical operations in support of criminal and intelligence investigations.

While ASD's primary mission is signals intelligence and support the Australian Defence Force, ASD has been called on to assist an expanding range of intelligence and law enforcement partners. As the cyber threat environment deteriorates, ASD will need to prioritise the application of its finite capabilities for use against nation-state actors.

Solutions

Immediate term (2023)

- **Task AFP to use its existing powers to proactively disrupt cyber crime.** AFP would lead this mission, while industry partners supply capabilities.

Short term (2024)

- **Government should develop a long-term investment plan for the AFP, Australian Criminal Intelligence Commission and other law enforcement agencies** to ensure they can continue to exercise their statutory functions with operational independence.

- **Government should prioritise updating legislation to ensure law enforcement and intelligence agencies have fit- for-purpose powers.** Modernising and consolidating Australia's electronic surveillance laws in a single *Electronic Surveillance Act* had bipartisan support under the previous government, but reform has stalled. Proposals for new ransomware and malware distribution offences should be refreshed.

Outcomes

- AFP polices cyberspace—just like it does for federal crimes on Australian soil—protecting Australians from harm.
- ASD is able to serve its core national security missions and optimise its REDSPICE transformation.

Act on victim reports to materially reduce high-volume cyber crime

The problem

While cyber extortion attacks gain significant attention and cause high-profile harm, Australia's economy and society is suffering deaths by a thousand cuts, with cyber-enabled crime affecting Australian citizens and businesses every day.

Today, the government *counts* high-volume cyber crime, but it urgently needs to *counter* it. ACSC have built a 'front door' for victims to report cyber crime – the ACORN system. They receive a report every 7 minutes. But there's only a nascent back-end to deal with the volume of reports. Most victim reports will not meet thresholds for police investigation.

This reflects policing of a pre-cyber era – now, one criminal can victimise thousands of individuals at a scale and speed previously unimaginable. Proper back-end analysis and linking of identities and common patterns will highlight the criminal groups preying on Australians and, importantly, can be shared with private sector organisations to protect future victims (for example, restricting money mule bank accounts and stopping scam emails and phone calls).

Solutions

Immediate term (2023)

- **Task the JPC3, and ensure it is appropriately resourced, to triage, corroborate and investigate victim reports** and can use this information to prioritise police activity and share with appropriate private sector organisations.

Outcomes

- The AFP identifies the criminals causing harm at scale – even if individual losses are relatively small.
- The AFP generates and shares intelligence with organisations that can protect Australians from cyber volume crime—banks, telcos, data centres.

3. Focus the market on improving Australians' cyber security

Overview

Cyber security is a whole-of-economy challenge, but a range of market failures and inefficiencies are holding us back. Most changes that need to happen for Australia to reach its ambition of most cyber secure country by 2030 will need to happen in the private sector. While government must lead on law enforcement and cyber crime disruption initiatives, when it comes to uplifting Australia's cyber resilience, the government's main role will be as a standards-setter and regulator. In considering how the government should do this, we urge the Expert Advisory Board to revisit Home Affairs' 2021 consultation, *Strengthening Australia's cyber security regulations and incentives*, and CyberCX's submission to that process.[1]

Mandate threat-blocking and secure-by-design practices from telecommunications and technology providers

The problem

Australians face an epidemic of scam texts, calls and emails, despite incremental steps by government. The digital services we use – from online banking to e-commerce platforms – also have no consistent security baseline. Recent regulatory changes, for example to enhance obligations to block spam or malicious text messages, are welcome. But efforts need to be bigger in scale and scope.

Large telecommunications, finance and digital service providers are uniquely positioned to detect and mitigate cybers threats due to the scale of the networks they operate and the customer base they serve. There are opportunities at different layers of the technology stack to block or disrupt threat actors and protect end users. For instance, the providers of operating systems, app-stores and social media platforms increasingly have the technical capacity to detect and block malicious actors. Currently, these entities engage in voluntary activities to address serious criminal activity on their networks. Enhanced vulnerability management, detection and response capabilities are also offered as premium service offerings. User equipment is also increasingly configurable to deliver protections for more vulnerable customers (such as children and older Australians) but this may not be activated 'out of the box'.

Solutions

Short term (2024)

- **Government should introduce legislation to require threat blocking at scale by telcos and ISPs.** Telstra has a nascent filtering capability to automatically block millions of malware communications on its infrastructure every week. This should be extended to all major telcos and ISPs across a broad spectrum of filtering types.

[1] https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/cybercx.pdf

- **Government should also consider legislation that incentivises or mandates ISPs to disconnect devices that are causing (or likely to cause) harm.** Without an owner's knowledge, an insecure device may be connecting to a threat actor's command and control infrastructure or spamming other network users. ISPs have exceptional network visibility. They should have the ability (and be incentivised to use it) to notify device owners of steps they can take to secure devices causing harm (such as downloading patches) and to disconnect them if they do not comply.

- **Government should create 'safe harbour' protections for telcos and technology companies that act in good faith, but act on false positives.** In a largescale threat blocking model, there will be false positives – but right now the government has got the balance wrong. Its risk aversion in not incentivising and/or mandating threat blocking at scale is harming Australians.

- **Government should introduce legislation to incentivise and in some cases mandate secure-by-design and secure-by-default settings**, and create clearer causes of actions for consumers who suffer harm when these standards have not been followed.

Outcomes

- Baseline security for every Australian internet and phone user is lifted.
- Law enforcement can focus on disrupting (and prosecuting) the most serious threats.

Enhance compellance powers, where users fail to address negative cyber externalities

The problem

Supply chain attacks are growing. Cyber insecure practice don't just harm individual organisations, but can cause cascading harm across the economy. For example, the ACSC estimates that up to 200,000 personal devices and routers in Australian homes and small businesses are vulnerable. These networks are weaponised by nation-states and cyber criminals, that use them as a vector to target other organisations.

Solutions

Short term (2024)

- **Government should consult on legislation to enhance government compellance powers.** This regime could include notices and advice, followed by compulsory disconnection for networks or devices that pose an unacceptable risk to the community.

Outcomes

- Businesses and individuals have more awareness and incentives to act to prevent their devices causing harm to others.
- Government has more ability to protect Australians from known threats.

Accelerate digital identity reform to reduce the harm caused by data breaches

The problem

A huge, growing amount of identity documents and other identify information is retained by public and private sector organisations. Almost all of the data breach incidents we responded to over 2022-23 involved identity documents and other personal information. This is a legacy problem that could be partly solved by a 21st-century approach to verifying information. Currently, Australia's digital identify verification options have low uptake and are not well understood.

Solutions

Immediate term (2023)

- **Accelerate the modernisation of Australia's digital identity processes,** so consumers and citizens can verify who they are without organisations capturing and storing this information.

Outcome

- Australia has a trusted and secure digital identity system, that citizens use instead of sharing identity documents or identity information with multiple private and public organisations.

Ensure Australia's privacy reforms incentivise data minimisation and protection, given Australia's deteriorating cyber threat environment

The problem

Australia's data protection and privacy standards are behind many of our peer democracies. Indeed, the European Commission does not consider Australia an 'adequate jurisdiction' for data protection when transferring personal data out of the EU, unless enhanced protections are in place. While this is a challenge being addressed under a separate reform process, CyberCX urges the government to closely align its privacy reform agenda with the realities of the deteriorating cyber threat landscape.

Cyber criminals understand the value of our personal information. In 2022, over 80% of cyber extortion cases investigated by CyberCX Digital Forensics and Incident Response experts involved a data theft extortion element. We have also observed an increase in attacks against small to medium businesses, not just large enterprises. Collecting too much data, without appropriate oversight and protection, increases Australia's attack surface and likelihood and impact of harm caused to Australians by cyber crime.

More than half of Australia's personal information handling is effectively unregulated, due to small business and employee record exemptions to the *Privacy Act*. In 2023 and beyond, the notion that small business data processing does not pose a significant risk to the community or that employee records shouldn't be given equal protection is outdated.

The government has yet to meaningfully tilt corporate incentives, so that data gluttony is not rewarded. Recent increases to penalties for misuse of personal information are welcome and will help the market to "price in" the risk of data misuse. But incentive structures could be further changed. Currently, the *Privacy Act* allows many businesses to collect information about Australians to support services which primarily benefit the business, such as their marketing and analytics functions or data monetisation programs, without getting meaningful, express and singular consent from individuals.

Solutions

Immediate term (2023)

- **Ensure that the current exemptions to the Privacy Act for small businesses and employee records are removed.** We note the Privacy Act Review Report released by the Attorney-General's Department in February 2023 made some proposals to remove these exemptions.

- **Ensure data minimisation by default**, including by making "opt in" for marketing and tracking the default setting for all Australians. In addition to reducing national cyber risk, a consent model for these types of activities is in line with what the community have asked for in multiple privacy surveys, such as the three yearly OAIC Australian Community Attitudes to Privacy Survey.

Short term (2024)

- **Significantly increase funding and change the long-term funding model for the privacy regulator**. Proposed regulatory changes will have little effect without significant change to the current resourcing of the OAIC. The Privacy Act Review does propose that further consideration be given to how to best do this. We urge the government to consider an industry-funded model, like that of ASIC or the Information Commissioner's Office in the UK, to ensure funding is proportionate to the volume of personal information processing that occurs nationally.

Outcomes

- The OAIC is appropriately funded and its capability scales with the growth of business.
- Australia has a world-leading privacy regime to meet community expectations and match our national ambition to be a cyber security world leader.

Review corporate governance rules and regulations relevant to cyber incidents

The problem

Increasingly, but not always, ASX-listed entities are disclosing cyber incidents to the market when they start a cyber incident investigation process. But there is confusion about what counts as a material incident, when disclosure should be made, and how. The market lacks an agreed framework to classify incidents based on seriousness and impact. There is also often a tension between market disclosures and communications to affected stakeholders, such as customers who have had their data stolen.

An incident response process usually takes weeks. Early disclosures can create confusion and uncertainty. There is tension between what a company knows at the beginning of a response and what it discovers as an investigation progresses and threat actor activities and objectives change. On average across CyberCX 2022 investigations, it took 15 days for a victim to even detect a data theft extortion incident. That's 15 days of threat actor activity the victim then needs to forensically reconstruct to understand what has happened. Organisations with faster detection times can also be punished by disclosure expectations. Companies must also grapple with the real-time adaptions of a threat actor which may still be in their network, and which monitors and responds to their public communications.

Solutions

Short term (2024)

- **The government, working with ASX, should consider guidelines for disclosing cyber incidents to the market.** These guidelines should focus on minimising harm to customers and other stakeholders, not just shareholders only.

Outcomes

- Market certainty about appropriate disclosures during cyber incidents.
- A disclosure regime that acts to minimise the harm of cyber attacks to the Australian economy and citizens.

4. A cyber workforce for the cyber century

Overview

Australia will not meet its cyber security objectives if it does not address its cyber workforce shortage. The September 2022 *Upskilling and Expanding the Australian Cyber Security Workforce* report,[2] developed with independent think tank Per Capita, makes it clear that:

- Over the next four years, the shortfall of qualified cyber security professionals is forecast to hit up to 30,000 unfilled positions across Australia.
- Women are wildly under-represented in the cyber workforce, clocking in at roughly 21 percent.
- Established training pathways through universities and TAFEs are unlikely, on their own, to deliver the required qualified graduates to the sector.
- Academy-style programs sponsored by cyber and technology companies show great promise in enabling additional pathways into the industry.
- Immigration must play a key role is closing the skills gap, alongside increased domestic investment.

Deliver value for money in government-supported cyber training, by targeting initiatives that deliver scale and are commercially viable

The problem

The government spends millions every year supporting the development of digital and cyber skills. Despite this substantial and growing investment, the cyber skills gap has continued to grow.

The 2020 Cyber Security Strategy introduced the $26.5 million Cyber Security Skills Partnership Innovation Fund (the Fund) to attempt to arrest the cyber skills shortage. While this investment was welcome and encouraged many new-comers to the cyber training space, particularly from industry where much of Australia's cyber know-how is located, the Fund's approach invests too broadly, across a smorgasbord of small, start-up style programs which do not offer the taxpayer sufficient value for money.

Solutions

Short term (2024)

- **The Fund – and future initiatives – should be redesigned to prioritise programs that can deliver:**
    - **Scalability,** to deliver significant numbers of cyber security professionals into the market.

[2] https://percapita.org.au/wp-content/uploads/2022/09/Upskilling-and-Expanding-the-Australian-Cyber-Security-Workforce-CyberCX-Branding-FINAL.pdf

- **Commercial viability**. Government should focus on projects that will not require permanent government funding, for example by prioritising commercial cyber security training entities that are designed to be commercially self-sufficient.
- **Likelihood of employment** for trainees. To do this, government should examine what gaps are most prevalent and persistent across the private and government workforces and calibrate support accordingly.

Outcomes

- A group of industry-led academy-style cyber training programs which operate at the scale required to deliver the better part of the 30,000 cyber security professionals Australia needs.
- Commercially viable programs that can continue to build the cyber workforce of the future without an endless tail of government subsidy.
- Real economic opportunities for Australians.

Create partnerships with industry to deliver on the REDSPICE ambition

The problem

At $9.9 billion, the REDSPICE initiative is the single most significant investment in ASD's history. The initiative aims to recruit 1,900 new analysts, technologists, corporate and enabling roles into ASD. Like all organisations and businesses across Australia, REDSPICE has struggled to attract the volume and quality of Australians with the requisite skills and security-appropriate background. ASD is not alone in this challenge. Several Australian companies have developed academy-style programs to address this same issue. These organisations have had to learn how to deliver training at scale, with graduates job ready from day one. Without both of these outcomes in industry, no program is able to survive. Government has an opportunity to lean on the hard-learnt lessons of industry and partner with companies that have an established track record of training cyber security professionals to job-readiness, at scale.

Solutions

Short term (2024)

- **ASD should partner with industry to identify, train and recruit cyber security professionals at scale.** This program should enable ASD to identify diverse talent and build employee pipelines through pre-training programs. Government should focus on companies that have already built scaled workforce solutions and understand ASD's unique security and cultural requirements.

Outcomes

- REDSPICE succeeds and delivers vital national security capability to Australia.
- Value for money, as industry training programs deliver workers below current costs borne by government.
- More cyber professionals are recruited into ASD, and faster, including diverse candidates who may not have previously considered working in the intelligence community.

Accelerate existing capability into the cyber workforce by removing workforce restraints

The problem

The majority of Australia's 30,000 cyber security workforce shortage will be addressed in coming years by training new-comers. But too much capability is being held back by existing workforce restraints, including:

- Complex or not-fit-for-purpose migration settings for skilled migrants.
- Security clearance delays, even for low-level security clearances, and difference, inefficient processes across federal and state governments and even within federal government.
- APS staff caps.

Migration

Australia needs to have a sensible conversations about the role that skilled cyber migration will need to play in closing the 30,000 worker shortfall that is forecast in the Per Capita *Upskilling and Expanding the Australian Cyber Security Workforce* report. While Australia cannot migrate our way out of this issue – particularly given our need to grow our sovereign workforce – it is clear that migration will play a role here. Unfortunately, too many cyber security professionals are caught in a migration system which has treated cyber security as an afterthought. To secure certain visa classes, applicants must demonstrate their ability against a set of criteria which too often bear little resemblance to their real-world role or capabilities.

Solutions

Immediate term (2023)

- **Home Affairs should review its classifications for cyber-related visas, as part of ongoing work to deliver the Commonwealth's new migration strategy**. This review should occur in partnership with industry, with opportunities for employers and employees to contribute.

Short term (2024)

- **Government must reform the security clearance process,** to speed clearance processes and reduce inefficiencies.

Longer term (2025+)

- **Remove the APS Staff Cap** to improve the capacity of departments and agencies to grow the government's cyber security workforce. This measure would also have flow-on benefits to the wider community, as professionals move in and out of government over their careers.

Outcomes

- Faster visa processing times deliver a bigger cyber workforce, faster.
- Security clearance processing improvements end recruitment bottlenecks.

- Public service cyber capability grows, particularly in non-REDSPICE departments and agencies, delivering value-for-money by reducing consultants 'body shopped' into government.

Develop accreditations for cyber security professionals

The problem

There are a range of cyber security accreditation and tertiary qualification systems. But they are often patchwork, occasionally inconsistent, and not always universally recognised. Many roles have no accreditations at all.

This accreditation gap presents challenges for employers, who have difficulties determining if candidates have the right skills. It also creates challenges for workers, who face barriers changing employers, as they cannot demonstrate in a standardised way what they are qualified to do.

There is also too much variability in the design of relevant tertiary programs. Students are graduating without the job-ready skills cyber employers need, often resulting in employers investing tens of thousands of dollars to close these gaps. Given the high subsidies given to cyber students for the cost of their education (which is ultimately borne by the taxpayer) more needs to be done to align these qualifications with real world requirements.

Solutions

Short term (2024)

- **Government should support the development of a more comprehensive and standardised framework for industry accreditation of cyber security professionals,** including both technical and non-technical roles**.**

Longer term (2025+)

- **Government should work with industry to create a peak-body** with an accreditations process tested by relevant agencies, academia, and industry.

- **Government should help tertiary degrees to become better aligned to national requirements,** focusing on essential areas of specialisation, whether it be cyber security theory, networking practices, penetration testing or governance, risk and compliance. For example, America's National Security Agency operates a National Centers of Academic Excellence in Cybersecurity program which accredits institutions for Cyber Defence, Cyber Research or Cyber Operations based on the contents and outcomes of their degrees.

Outcomes

- Employers more able to recruit the skills they need.
- Workers can more easily change employers and pursue different career pathways.
- Australia has nationally-consistent benchmarks to inform the design of courses and professional development programs.

5. Elevate Australia's international cyber leadership

Overview

Australia can have its most meaningful impact on international cyber resilience by focussing on our Pacific and broader Southeast Asia neighbourhood and continuing to advocate for Australia's interests in like-minded groupings.

Work through larger multilateral organisations, including on standard-setting and norm building is necessary and must continue – but is unlikely to deliver the outsized return on investment that Australian leadership in our region and via select diplomatic and operational groupings will.

Bolster cyber capabilities for, and through, AUKUS

The opportunity

AUKUS pillar two – concerning technology co-development between the US, UK and Australia – offers historic opportunity to Australia and could deliver security dividends much faster than pillar one (related to undersea technology). To unlock the benefits of pillar two, which expressly contemplates building cyber security capability, requires creative diplomacy and leadership from Australia. It will also require a compact between government and industry, and for Australia to demonstrate high levels of national cyber resilience so our partners have the confidence to share their most coveted intellectual property.

Solutions

Immediate term (2023)

- **The Cyber Security Strategy should commit to developing a plan, with industry, for how Australia's leading cyber firms can be incorporated into AUKUS planning and activities.**

Short term (2024)

- **The government should identify roadblocks to deeper industry-industry and government-industry collaboration across AUKUS countries** and spearhead a diplomatic campaign to stimulate change in the US and UK to address these roadblocks.

Outcomes

- Industry, which is where much of our cyber capability innovation will occur, meaningfully participates in AUKUS.
- Australia unlocks the full potential of the historic AUKUS security partnership, by advocating for and facilitating joint cyber capability projects.

Focus international engagement on the Pacific and Southeast Asia, delivering safer infrastructure and practical capability

The opportunity

As Australia strives to be the world's most cyber secure country by 2030, we must not leave our neighbours behind. Since our first international cyber engagement strategy, Australia has delivered regional investment initiatives, capability building and aid programs. This should continue and deepen.

The Cyber and Critical Tech Cooperation Program (CCTCP) has been an essential vehicle for uplifting cyber security and capability across Southeast Asia and the Pacific. There are opportunities to make these efforts even more practical and operationally-informed. Recent efforts of security experts and diplomats to support major cyber incident responses on the invitation of Pacific countries highlights the benefits of industry involvement in Australia's international engagement. Further, recent efforts such as the Coral Sea Cable and Telstra's purchase of Digicel Pacific show how supporting foundational communications and cyber technologies in our region can uplift economies and ensure greater collective security.

Longer term, Australia is in a mature position to develop competitive cyber security education offerings for Southeast Asia and the Pacific. Education is already Australia's largest service export. As we refine our educational offerings to meet domestic demand, our region can also benefit.

Solutions

Immediate term (2023)

- **The Cyber Security Strategy should commit to more investment in digital infrastructure and cyber capability in our region** via the CCTCP and like initiatives. In this, the government should focus on practical training and operational support initiatives alongside industry, including incident preparedness, response and remediation.

Longer term (2025+)

- **The government should build towards a vision of making Australia a regional cyber knowledge hub,** leveraging efforts to professionalise and grow our domestic cyber workforce. This initiative would also deepen person-to-person ties and practical collaboration between neighbours.

Outcomes

- Australia acts as a regional leader in cyber security and the roll-out of safe and secure digital infrastructure across our region.
- More industry involvement in Australia's international engagement unlocks more benefit and uplift for Southeast Asian and Pacific partners.

CyberCX

About CyberCX

The greatest force of cyber security experts

CyberCX is a global cyber security company comprising highly skilled consultants, capabilities and offices in Australia, New Zealand, the United Kingdom, and the United States. With a workforce of over 1,300 professionals, we are a trusted partner to private and public sector organizations helping our customers confidently manage cyber risk, respond to incidents, and build resilience in an increasingly complex and challenging threat environment.

Through our end-to-end range of cyber capabilities, CyberCX empowers our customers to securely accelerate opportunities in the digital economy.

Our expertise is delivered across the following services:

- Consulting and advisory
- Governance, risk, and compliance
- Incident response
- Penetration testing and assurance
- Security integration and engineering
- Cloud and identity security
- Managed security services
- Cyber security training

Led by industry experts and delivered by cyber security specialists committed to their craft, CyberCX represents the region's best cyber security talent, applying unmatched cyber security expertise to protect and defend both local and international organisations from cyber threats.