Australia National Cybersecurity Strategy

Matthew Rosenquist
CISO & Cybersecurity Strategist

Executive Overview:

Australia is pursuing a bold vision to become the world leader in cybersecurity by 2030.

There has been no national cybersecurity plan or strategy that has been wholeheartedly lauded as an overwhelming success by any government. Therefore, completing this endeavor requires significant thought leadership. Many governments have pursued a similar initiative to some extent, but the results vary greatly in effectiveness and sustainability.

In early 2023, the Minister for Cyber Security, the Hon Claire O'Neil MP appointed an Expert Advisory Board who has reached out to the global cybersecurity community to solicit ideas on how the government can achieve its vision to and protect their national interests, citizens, and economy.

This paper is in response to the request for constructive inputs for consideration to assist Australia in achieving its goals.

The paper outlines:

1. The need for a cohesive, strategic, and well-thought-out plan.
2. Principle areas that are necessary for a successful national-level strategy.
3. Initial recommendations of action in each area as part of a strategic plan. (not all recommendations are required)
4. The requirement for continuous forethought, planning, and operational excellence for sustainability.

Also included is **APPENDIX A**, a list of questions included in the 2023-2030 Australian Cyber Security Strategy Discussion Paper and my corresponding answers/recommendations that are highlighted in this paper.

A Strategic Plan

A successful strategy is stronger than the sum of its individual parts.

The problem to overcome is multifaceted. Cybersecurity has often been miscategorized as solely a technical issue, one which has eluded being solved for decades even with massive amounts of engineering innovation being applied. The reality is there are regulatory, economic, behavioral, social, and intelligent-adversarial aspects that add significant complexity that technology alone cannot fix.

Additionally, trying to attack the problem with a piecemeal approach with discrete independent functions or achievements, no matter how impressive, cannot overcome the momentous and dynamic challenges that Australia will face in the future.

No amount of point solutions will solve the systemic problems at a national level. In fact, adding too many solutions can increase the complexity and undermine the sustainability of managing security risks.

Australia's strategy must carefully curate a set of mutually reinforcing frameworks, capabilities, and direct actions that elevate the overall ability of a country to manage its cybersecurity risks across its government, critical infrastructures, business economy, and citizens.

It is no easy task. The development of cybersecurity strategies at a much smaller level, that of corporations, is also fraught with difficulties, but one thing is for certain - cybersecurity for sizeable or complex organizations will fail without an overarching strategy. (Additional reading: Cybersecurity Fails without Strategy) The same is true for the larger scope and more complex goal of protecting a nation.

National-level strategies have the advantage of potentially addressing or positively influencing all aspects that hold back cybersecurity. However, there must be a thoughtfully designed set of governance, investments, and prioritized actions that integrate in particular ways to achieve several objectives in coordination and produce more powerful overall outcomes.

Strategic Principles for Success

All the following strategic principles represent fundamental domains that must be crafted to work together collaboratively for a national-level cybersecurity strategy to be successful. Absence or apathetic effort in any one of the five primary principles will likely undermine the remaining efforts and become the catalyst for long-term failure.

1. **Cybersecurity Leadership** for adaptability attunement, planning, oversight, and superb execution
2. **Regulatory Frameworks** and laws to establish governing policies applicable to domestic entities and foreign collaborative agreements
3. **Risk Controls** to be implemented, sustained, and innovation to support adaptation, both proactive and reactive, across technology, behaviors, and processes
4. **Targeting Attackers** – actions to remove, block, or demoralize/deter those with the intention of doing harm, to stop attacks at their origins before harm is done
5. **Cooperation & Enablement Cohesion** – to amplify effectiveness and sustainability through communication, public/private partnerships, growth of the cybersecurity industry capacity, and leveraging international coalitions for standards, technology supply-chain, intelligence sharing, and threat-targeting collaboration

Principle Stratagems:

1. **Cybersecurity Leadership:** Great leaders have often been the key to the success of great endeavors as they model professionalism in their work, capitalize on available resources, bring cohesion among teams, motivate through common goals, find creative solutions, and inspire others to do the same. Cybersecurity represents a number of significant challenges in many different disciplines. Australia must elevate brilliant leadership at all crucial levels to organize, defend, proactively adapt, and inspire teams based on experience, professionalism, and skill. Not every organization needs a superstar leader in every role, but the absence of real leadership can doom even the most competent and capable security initiative. In the worst case, an incompetent leader can cause more harm than good. (Additional reading: When the Wrong Person Leads Cybersecurity)
2. **Regulatory Frameworks:** Regulatory and policy frameworks establish a common ground, minimum requirements, and a common language of terms that unifies various organizations and even competitors. In cybersecurity, regulations 'raise all boats' to a minimum acceptable level of risk management, thereby reducing the overall range of disparity. Regulatory compliance is a launching point where investment in cybersecurity

can evolve to be a competitive advantage and drive innovation. Unfortunately, there is no one common set of rules that are equally applicable across the sectors and vast use cases. Therefore, Australia must establish regulatory frameworks that set conditions to unify defense initiatives, set guardrails for effectiveness, streamline potential conflicts, and minimize overall potential impacts specific to use-case archetypes and business sectors. Deriving the frameworks can be complex and must take into account the threat actors, inherent risks exposures of necessary functionality, the likelihood of attacks, and overall probable impacts. A coalition of experts across public and private sectors, guided by national-level strategic goals, would be well-positioned to define and strategically maintain balanced and effective regulatory frameworks.

3. **Risk Controls:** Controls are a combination of technology, behaviors, and processes which mitigate in proactive/reactive ways or transfer cyber risks. Controls become stale and lose effectiveness over time. Support for innovation, the establishment of best practices, the pursuit of effectiveness, and operational excellence are key. Automated and intelligent controls allow for risk mitigation across vast digital landscapes in affordable ways. The most popular controls continue to be technical, which maximize the advantages of defending the technology battlefield, by preparing it properly to be disadvantageous to the attackers. In reality, many layers and types of controls are necessary to thwart sophisticated attacks.
4. **Targeting Attackers:** Threat Agents, those who act and support digital attacks, are the origins of risk. They are the starting point of cybersecurity and by undermining their motivation, constricting their capabilities, or removing them as a threat, the risks can be diminished greatly at scale. Targeting the attackers can be the single most cost-effective way of improving digital security and aligns with social norms and infrastructure for maintaining a safe society.
5. **Cooperation, Enablement, & Sustainability Cohesion:** Maneuver for long-term success by investing or facilitating innovation, raising the cybersecurity 'common sense' savvy of every citizen, implementing digital ethics, establishing workforce pipelines to support the security industry, conducting effective communication and awareness, and leveraging international collaboration.

Recommendations for Key Initiatives & Actions:

1. Cybersecurity Leadership

Expert leadership is key to driving specific areas for advancement in cybersecurity and overcoming the inherent chaos, ambiguity, and challenges of outmaneuvering an intelligent adversary and evolving computing environment.

Objective: The placement and sustainment of cybersecurity leaders in key government positions, business sectors, legislative, regulatory, judicial, and law enforcement should be a driving force that collectively and collaboratively tackles legacy and emerging cybersecurity problems for the betterment of Australia's government, businesses, and citizens. This includes proper candidacy selection for positions, additional training, mentorship, and

continuous education for those leaders.

Specific Initiatives to ensure excellent cybersecurity leadership representation is in place:

1.1. Australian government:
  1.1.1. Australian Ministry of Cybersecurity – top leadership and accountability
  1.1.2. Australian Cybersecurity Expert Group – Primary group to advise the Minister for Cyber Security
  1.1.3. Global Advisory Board – experts in their fields to supplement and advise the Australian Cybersecurity Expert Group
  1.1.4. Cybersecurity Diplomats/Foreign Communication and Advocacy must establish delicate agreements
  1.1.5. Cybersecurity heads are responsible for protecting specific branches and agencies

1.2. Sector Leads – Each business sector, especially critical infrastructures and government agencies, requires strong leadership to define risk models, 'best practices', lead information-sharing forums, and minimum-security standards. SMBs, as a community, also need expert leadership representations.

1.3. Legislative branch – to lead the timely creation of laws and regulations in support of cybersecurity

1.4. Regulators – Regulatory bodies need leadership to establish effective auditing processes and accurate reporting of violations

1.5. Law Enforcement – to develop capabilities in local, national, and in partnership with international law enforcement, to investigate criminal actions and prepare proper cases for prosecution

1.6. Judicial branch – Leadership will be needed to interpret the laws, rule over challenges to regulations, determine liability, and understand the nuances of criminal cases in just and consistent ways.

1.7. Innovation incubation – Perhaps one of the most important aspects is to attract innovation leaders to develop and bring to market new cybersecurity tools, products, and services.

1.8. Technology risk oversight – Understanding the risks is one of the most difficult aspects of cybersecurity. There needs to be a national group or think tank to understand how the national strategy is working or needs improvement. This team will also work with international partners.

1.9. Establish an international Cybersecurity Advisory Board of recognized experts to help continually plan, test, refine, and evaluate cybersecurity initiatives, who are:
  1.9.1. Successful in establishing and managing cybersecurity capabilities at a business, sector, or governmental branch level
  1.9.2. Thought leaders that have established or defined effective and timely cybersecurity industry best-practices
  1.9.3. Cybersecurity strategists with a proven record of predicting emerging threats and proactive counters

1.10. Direct and empower government cybersecurity leadership (Expert Group and Advisory Board) to work in conjunction with private sector leaders to:
    1.10.1. Develop specific plans to address pressing tactical problems: (ransomware, vuln exploitation, supply chain attacks, critical infrastructure resistance/resilience, etc.)
    1.10.2. Craft a broad and holistic risk assessment framework for critical national systems, analyze the results, and provide recommendations that leverage the 5 tenants of this cybersecurity strategy to erect the strongest defenses where needed. Critical targets must be better defended and controls implemented as a priority.
    1.10.3. Prioritize direct investment to the most critical areas of potential impact (weighted protection)
    1.10.4. Identify creative approaches to undermine the attackers' fundamental advantages
    1.10.5. Identify areas to commit indirect investment to raise the overall security levels of the community (raise all boats)
    1.10.6. Identify short-term specific ways to reduce the perception and reality that Australian citizens, businesses, and organizations are 'Easy Targets' as compared to other nations
1.11. Establish a cybersecurity auditing capability that reports findings to a centralized office for critical sectors at a minimum
1.12. Establish a centralized cybersecurity metrics reporting and aggregation group for each critical sector to identify trends, issues, and best practices that will disseminate key findings to that sector and the centralized auditing or intelligence group
1.13. Promote Australian thought-leaders as top cybersecurity communicators and industry influencers

2. Regulatory Frameworks

Government regulations must be enacted to drive minimum standards and to hold accountable any parties which choose to undermine cybersecurity to the detriment of citizens and other organizations.

Objective: Establish mutually supporting regulations to facilitate predictive, preventative, detective, and responsive cybersecurity capabilities across technology, people, and processes. This includes minimum standards, liability responsibility, blocking criminal benefits, facilitating criminal investigations and prosecutions, and allowing the seizure of assets in support of digital criminal activities.

Specific Initiatives for regulations and laws to be created or improved:

2.1. Minimum security controls by sector, i.e. cybersecurity basics with compliance requirements and penalty structures for non-compliance
2.2. Legislation specifically mandating that all Critical Infrastructure organizations, and their supply chains, meet a minimum standard for cybersecurity protection

(prevention, detection/response, resilience/recovery) - each sector will have a section lead to define the specific requirements, with the assistance of the Advisory Board

2.3. Reporting and transparency of risks, attacks, and security posture compliance
2.4. Requiring victim and shareholder notification in the event of a breach, exploitation, or incident that undermines the confidentiality, integrity, or availability of systems or data.
2.5. Minimum controls and attestation for national Critical Infrastructure products, services, and operations.
2.6. Regulation mandating that no aid or support will be provided to the enemy/attackers. This includes ransoms and payments to digital extortion. Make it a criminal offense.
2.7. Supply chain security requirements for hardware, firmware, software, services, and devices
2.8. Digital ethics/privacy transparency and accountability
2.9. Define how Australia wants to proactively and reactively disrupt and dismantle threat actors, with proportional or disproportional force, and if diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement instruments will be involved (ex. US National Cybersecurity Strategy).
2.10. Regulations requiring compliance to cross-national agreements and cooperation for sector standards, criminal investigations, real-time threat data, risky product bans/embargos, and metrics information sharing
2.11. Establishing manufacturer/vendor liability for insecure products and services, and poor cybersecurity practices
2.12. Mandate zero-vulnerability product release, functionality for patch/fix/recover architectures, and active product patching capabilities by vendors/manufacturers for systems involved with sensitive public data, services, or capabilities that citizens are reliant upon
2.13. Require a process for continual identification of fundamental security architecture investments and compliance expectations for national critical infrastructure sectors (ex. Zero Trust, MFA, Asset tracking, resilience, and BCDR)
2.14. Cryptocurrency regulation for centralized exchanges/service providers, onboarding/offboarding to international currencies, and fraudulent mis/disinformation to counter cybercriminals using these capabilities for money laundering
2.15. Incentivize cyber insurance to require specific minimum-security practices of clients before issuing a policy
2.16. Specify parameters for the government and courts to seize digital infrastructures and assets which directly or knowingly support criminal activities
2.17. Cooperate and support international efforts to track decentralized cryptocurrency accounts and transfers which are associated with illicit activity
2.18. Clarify laws governing cybercrimes, prosecution, and punishments for improved law enforcement effectiveness
2.19. Clarify laws and penalties for organizations failing to meet standards for protection, reporting, cyber-ethics, privacy, and international agreements for improved regulatory compliance effectiveness
2.20. Pass legislation to place accountability on vendors and their executives/boards for the security of their products, services, and operations

3. Risk Controls

Controls mitigate risks and must be applied in smart ways and continually tuned to remain effective. Australia must influence, promote, and incentivize the development and integration of innovative technology, behavioral, and process controls to mitigate cyber-attack risks effectively and efficiently across organizations and over time.

Objective: Lead the industry in establishing well-suited standards, expectations, and best practices for cybersecurity controls. Establish government-led communications, alerting, and information assessment capabilities as a public resource to improve cybersecurity practices. Set market expectations for vulnerability and patching. Define clear architectures and standards requirements for government and all critical infrastructure entities.

Specific Initiatives to drive the continuous improvement of technical, behavioral, and process controls:

3.1. Defining, maintaining, and communicating 'cybersecurity best practices'
3.2. Identifying and communicating shifting threat agent tactics, tools, and procedures
3.3. Investing in private-sector cybersecurity innovation and Australian cybersecurity start-ups
3.4. Tracking vulnerability to mitigation/patch availability and adoption timelines
3.5. Designing a national infrastructure for cyberattack detection, tracking, and interdiction (in cooperation with national critical infrastructure sectors)
3.6. Define frameworks for developing measurable risk goals
3.7. Both limit and encourage cybersecurity insurance for the transfer of high-impact/low-likelihood risks
3.8. Incentivizing realistic, comprehensive, and easy-to-use risk assessments that are common in scope, process, and ease of comprehension
3.9. Improve governments posture and security programs
3.10. Incentivize SMBs and enterprises to pursue optimized cybersecurity plans by working with the industry to develop customized planning tools (balancing risk, costs, and business friction)
3.11. Create standards to make technology significantly less vulnerable to exploitation
3.12. Create mechanisms to address supply chain weaknesses and minimize cascading failures
3.13. Government systems security options/recommendations:
    3.13.1. Limit Internet access by design. Compartmentalization of systems
    3.13.2. Whitelisting model for computers and applications
    3.13.3. RBAC controls, audits, R&R, and accountability
    3.13.4. Effective employee training
    3.13.5. Vendor vetting and liability
    3.13.6. Implement MFA for system, application, cloud, and data-store access
    3.13.7. Robust onboarding/offboarding process to revoke access and recover systems/data/assets

3.13.8. Insider cyber risk program
3.13.9. Realtime or near-realtime detection systems
3.13.10. Crisis response and recovery capability
3.13.11. External pen-testing, auditing, and expert consulting assessments

4. Targeting Attackers

Cyber risks originate with the attackers and directly targeting them has a powerful impact on the overall risk environment. It is extremely efficient and effective to directly engage with the threat actors, rather than with the methods they employ.

Objective: Find ways to remove, block-at-scale, or undermine the attacker's motivation. Raise the risks they personally face. Applying pressure at the source of attacks can be the most cost-effective means to impact the risk calculus.

Specific Initiatives to target attackers:

4.1. Pursue and prosecute attackers to remove them as participants from the field
- 4.1.1. Elevate law enforcement tools, processes, and capacities to effectively investigate and prosecute offenders
- 4.1.2. Establish a national cybersecurity law enforcement team to lead high-profile criminal cases, establish forensics capabilities, define clear processes of operation, and teach local law enforcement to facilitate or conduct their own investigations investigation, forensics, and prosecutions
- 4.1.3. Work to incarcerate and establish limits on convicted felons' access to digital systems or data. (see the related regulation recommendation, as it is a dependency)

4.2. Block major avenues of attack or exploitation, denying them infrastructure, tools, and techniques. Target single points of failure across technology, behaviors, or processes.
- 4.2.1. Direct the Expert Group and Advisory Board to work in conjunction with private sector leaders to create plans:
  - 4.2.1.1. Drive improvements to Identify and Access management, starting with weak credential security (ex. passwords), adoption of strong 2FA or MFA
  - 4.2.1.2. Patch prioritization efficiency frameworks coupled with standards for patch implementation timelines
  - 4.2.1.3. Recommendations for the adoption of Zero Trust architecture
  - 4.2.1.4. Mitigation of malicious use of AI in fraudulent activities like phishing, masquerading/impersonation, and forgeries. This may include aspects of new regulations and technology innovation.
- 4.2.2. Reinforce the incentivization of responsible reporting of vulnerabilities, to minimize the available 0-days
- 4.2.3. Pursue with vigor organizations which knowingly provide services and support for criminals (ex. Computing infrastructure, hidden domain ownership, money laundering services, social media accounts to sell/market illicit wares and

intimidate/harass victims). Invoke financial penalties and potentially criminal charges.

4.3. Demotivate, deter and dissuade potential threats to not conduct attacks

4.3.1. Undermine Ransomware as an attack vector by making digital extortion payments illegal and denying the perpetrators their reward, thereby demotivating them from future ransomware attacks against Australian targets (see the related regulation recommendation, as it is a dependency). *– For more information on the strategy to end ransomware in this manner, watch the How to End Ransomware video. Additional content on this topic can be found in the Ending Ransomware playlist*

4.3.2. As a deterrent, publicize the prosecution of cyber criminals, an international collaboration to bring suspects to justice, and subsequent punishments of convicted criminals

4.3.3. Pursue high penalties and broad seizure of assets (including computing infrastructures) to demotivate attackers and other persons/organizations who knowingly support or enable cybercrime

4.3.4. Promote whistleblowing and reporting with financial incentives, a percentage of the penalties recovered from convicted criminals, and related support structures

5. Cooperation, Enablement, & Sustainability Cohesion

Cybersecurity must maintain pace with the rapid evolution of threats, their methods, and the tools they employ. It must be sustainable over time. Capabilities must be operated, improved, and adapted in a timely, effective, and efficient manner. This includes keeping people informed and collaborating, technology updated and adopting new innovations, and updating processes for consistency and comprehensiveness over time. Cybersecurity innovation investment must be fostered and the establishment of a necessary workforce encouraged. Lastly, it is important that regulations are followed, offenders are pursued, and a strong culture of cybersecurity is continually promoted.

Objective: Facilitate strong public and industry communications, collaboration, and efforts that promote sustainable innovation, workforce development, operating metrics, threat intelligence, shared key learnings, and strategic modernization investment.

Specific Initiatives for the management and continuous improvement of cooperation, enablement, and sustainability cohesion:

5.1. Influencing whistleblowing of illegal, unethical, or non-compliant cybersecurity practices

5.2. Establishing a cybersecurity risk metrics dashboard

5.3. Sponsoring public cybersecurity research

5.4. Prepare the next generation of cybersecurity professionals (sustainability of talent)

5.4.1. Supporting STEM and Cybersecurity education programs

5.4.2. Supporting cybersecurity boot camps and degree programs

5.4.3. Certifying cybersecurity education standards

5.5. Establish a national civic education campaign to promote a culture of savvy cybersecurity by communicating:
    5.5.1. The relevance of security, privacy, ethics, and safety for digital systems
    5.5.2. The best practices that every Australian can benefit from, to improve behaviors and awareness of citizens, SMBs, enterprises, and organizations
5.6. Establish a national cybersecurity job placement/information site and integrate it with other nation's sites (ex. https://www.cyberseek.org) to facilitate talent growth, internships, education, job placement, and career advancement
5.7. Develop or join international coalitions for:
    5.7.1. Joint intelligence and alerting
    5.7.2. Technology supply-chain access
    5.7.3. Attacker tactics and techniques real-time alerts
    5.7.4. Shared R&D investments for technology, threat insights, cost reduction opportunities, and optimal security sustainability
    5.7.5. Joint criminal investigations
    5.7.6. Cybercrime infrastructure interdiction and asset seizure
5.8. Promote public/private partnerships that establish long-term improvement capabilities (standards, consortiums, collaborations, etc.)
5.9. Maintain visibility to the public, senior levels of government, and international partners through social media, marketing, and evangelists
5.10. Identify and commit indirect investment to maintain security sustainability
5.11. Establish sector relevant Incentives/Disincentives for elevated security posture and maturity levels in non-critical domains
5.12. Clearly define industry roles, responsibilities, and generic templates for service-level-agreements for the public and private ecosystem
5.13. Establish public/private fusion centers for bidirectional information sharing on threats, vulnerabilities, exploitations, and best practices in a timely manner
5.14. Establish a national public training campaign to communicate the importance of cybersecurity, improve users' behaviors, draw interest into STEM/Cybersecurity jobs, and promote the pursuit of those conducting attacks
5.15. Establish a political body to promote international cooperation for cybersecurity, cybercrime prosecution, community outreach/education, and international protection standards

Author:

Matthew Rosenquist

- CISO, Industry Cybersecurity Strategist, and Advisor

Matthew Rosenquist is the Chief Information Security Officer (CISO) for Eclipz, the former Cybersecurity Strategist for Intel Corp, and benefits from over 30+ diverse years in the fields of cyber, physical, and information security. Matthew is very active in the industry and advises fellow CISOs, boards, academia, governments, and businesses around the globe.

Matthew specializes in understanding the fundamental factors that drive and shift the industry. He has been providing cybersecurity predictions for decades, awarded many recognitions, and his insights have been published in reports from McAfee and a multitude of industry periodicals. As a veteran cybersecurity strategist, he identifies emerging risks and opportunities to help organizations balance threats, costs, and usability factors to achieve an optimal level of security.

He develops successful security strategies, measures value, develops best practices for cost-effective capabilities, and establishes organizations that deliver optimum levels of cybersecurity, privacy, governance, ethics, and safety. He is a member of multiple advisory boards, an experienced keynote speaker, publishes acclaimed articles, white papers, blogs, videos, and podcasts on a wide range of cybersecurity topics, and collaborates with partners to tackle pressing industry problems.

Follow Matthew on **LinkedIn** and watch his podcast, interviews, and videos on the YouTube **Cybersecurity Insights** channel.

APPENDIX A

Consolidation of the questions for consultation in the 2023-2030 Australian Cyber Security Strategy Discussion Paper and includes further specific detail.

Respondents may make a submission regarding the entire discussion paper and full list of questions, or select only those questions which are most relevant.

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?

A cohesive plan that reaches the breadth and depth of the long-term goals. By 2030 Leadership appointments, Cyber Workforce improvements, foundational regulations/laws, measures/metrics for goals and frameworks for inter/intra government collaboration should be in place.

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

Roles, responsibilities, accountability, and success/failure criteria for leadership are all crucial to uplevel security and benefit a digital economy.

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

Security fundamentals as a baseline, with each sector having a minimum level/set of controls. Government and a few other crucial sectors must have a higher degree of specificity across legislation requirements, regulation limitations, and what is considered best-practices.

b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of ‘critical assets’ so that customer data and ‘systems’ are included in this definition?

More reforms are needed to include and show connections between critical assets, customer data, systems with access, supply chain vendors, user portals, security controls/oversight and systems facilitating rapid detection/recovery from attack.

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

There must be very clear expectations as related to fiduciary responsibilities. This must include cybersecurity expertise in the Board and a regular review of cybersecurity issues, metrics, and expected future risks.

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

Yes, several potential regulations are applicable and beneficial to establishing systemic protections for users, systems, data, and supply chains. See the Regulatory Frameworks section (Principle #2).

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?

First, leverage the Cybersecurity Expert Group and International Advisory Board to develop success/failure measures and metrics to understand the burdens. (Principle #1)

Use the proposed communication and public/private forums (Principle #5) to maintain continuous feedback and insights from the community.

This is where having a carefully crafted set of mutually supporting regulations is key to being comprehensive but not overly burdensome.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:

YES! See section on Targeting the Attacker (Principle #4). I reference a video where I outline a comprehensive strategy for undermining ransomware as an entire class of cyber attack. It does require the criminalization of paying ransoms or extortion, this would also prohibit insurers. It is a multi-year transition play but will satisfy the 2030 goal.

(a) victims of cybercrime; and/or
(b) insurers? If so, under what circumstances?

What impact would a strict prohibition of payment of ransoms and extortion demands by cybercriminals have on victims of cybercrime, companies, and insurers?

The adverse impacts can be mitigated. See the links I included to previously published videos in the Targeting the Attacker section. (Principle #4)

g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Absolutely! This must be tied to proposed regulations, community outreach, communication campaigns, and the other plans already documented elsewhere. See the links I included to previously published videos in the Targeting the Attacker section. (Principle #4)

3. How can Australia, working with our neighbors, build our regional cyber resilience and better

respond to cyber incidents?

Fusion centers, coordinated incident response, shared intelligence, formal agreements, and establishing working groups (See Section on Cooperation, Enablement, & Sustainability Cohesion. Principle #5)

Additionally, add regulations requiring compliance to cross-national agreements and cooperation for sector standards, criminal investigations, real-time threat data, risky product bans/embargos, and metrics information sharing. (See Section on Regulations. Principle #2)

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

Reference Section on Cooperation, Enablement, & Sustainability Cohesion. Principle #5

- 5.7 Develop or join international coalitions for:
  - 5.7.1 Joint intelligence and alerting
  - 5.7.2 Technology supply-chain access
  - 5.7.3 Attacker tactics and techniques real-time alerts
  - 5.7.4 Shared R&D investments for technology, threat insights, cost reduction opportunities, and optimal security sustainability
  - 5.7.5 Joint criminal investigations
  - 5.7.6 Cybercrime infrastructure interdiction and asset seizure
- 5.13 Establish public/private fusion centers for bidirectional information sharing on threats, vulnerabilities, exploitations, and best practices in a timely manner
- 5.15 Establish a political body to promote international cooperation for cybersecurity, cybercrime prosecution, community outreach/education, and international protection standards

5. 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 behavior in cyber space?

Lead the world in building and documenting the ‘How-To’ framework for an effective national cybersecurity capability!

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

First, empower departments with strong cybersecurity leaders. (Principle #1) Also, leverage the Cybersecurity Expert Group and International Advisory Board to guide departments and agencies to successfully implement and showcase best practices. (Principle #1). Then use public communication and outreach in the Section on Cooperation, Enablement, & Sustainability Cohesion. (Principle #5) to showcase thought leadership and operational excellence!

7. What can government do to improve information sharing with industry on cyber threats?

See all recommendations in the Section on Cooperation, Enablement, & Sustainability Cohesion. (Principle #5)

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organizations that experience a cyber incident so as to allow information to be shared between the organization and ASD/ACSC without the concern that this will be shared with regulators?

Information sharing is valuable during an incident in two ways: first as step to reach out for assistance and second as part of the ethical notification to partners, customers, and shareholders. The first must occur earlier. It may not be optimal for ASD/ACSC to be involved with every breach. Instead, it would be better for the commercial sector to reach out to local/national law enforcement agencies that are enabled and capable of assistance.

References:

1.5. Law Enforcement – to develop capabilities in local, national, and in partnership with international law enforcement, to investigate criminal actions and prepare proper cases for prosecution

2.9. Define how Australia wants to proactively and reactively disrupt and dismantle threat actors, with proportional or disproportional force, and if diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement

2.18. Clarify laws governing cybercrimes, prosecution, and punishments for improved law enforcement effectiveness

4.1. Pursue and prosecute attackers to remove them as participants from the field

4.1.1. Elevate law enforcement tools, processes, and capacities to effectively investigate and prosecute offenders

4.1.2. Establish a national cybersecurity law enforcement team to lead high-profile criminal cases, establish forensics capabilities, define clear processes of operation, and teach local law enforcement to facilitate or conduct their own investigations investigation, forensics, and prosecutions

5.15. Establish a political body to promote international cooperation for cybersecurity, cybercrime prosecution, community outreach/education, and international protection standards

9. 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?

Possibly, but the real value of notification is to facilitate victims in taking timely measures to

protect their identity and assets from further victimization and cascading attacks, including fraud.

Reference:

2.3. Reporting and transparency of risks, attacks, and security posture compliance

2.4. Requiring victim and shareholder notification in the event of a breach, exploitation, or incident that undermines the confidentiality, integrity, or availability of systems or data. 2.8. Digital ethics/privacy transparency and accountability

2.19. Clarify laws and penalties for organizations failing to meet standards for protection, reporting, cyber-ethics, privacy, and international agreements for improved regulatory compliance effectiveness

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

Varies. Intelligent attackers adapt to the effective practices of the defenders. A more strategic and holistic approach is required.

Reference:

1.1. Direct and empower government cybersecurity leadership (Expert Group and Advisory Board) to work in conjunction with private sector leaders to:

1.1.1. Develop specific plans to address pressing tactical problems: (ransomware, vuln exploitation, supply chain attacks, critical infrastructure resistance/resilience, etc.)

1.1.2. Craft a broad and holistic risk assessment framework for critical national systems, analyze the results, and provide recommendations that leverage the 5 tenants of this cybersecurity strategy to erect the strongest defenses where needed. Critical targets must be better defended and controls implemented as a priority.

1.1.3. Identify creative approaches to undermine the attackers' fundamental advantages

Defining, maintaining, and communicating 'cybersecurity best practices'

1.1. Designing a national infrastructure for cyberattack detection, tracking, and interdiction (in cooperation with national critical infrastructure sectors)

1.2. Create standards to make technology significantly less vulnerable to exploitation

1.3. Create mechanisms to address supply chain weaknesses and minimize cascading failures

Also see Section/Principle #1, Section/Principle #3, Section/Principle #4, and Section/Principle #5 for more intersects to address and manage risks of this challenging problem.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's

broader STEM agenda?

Yes, but it depends on your overall goals of people, skills, time into market, and the strength of the workforce development channel.

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

See recommendations in the Section on Cooperation, Enablement, & Sustainability Cohesion. (Principle #5)

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

Better communication, explanations, mapping to SLA expectations, and perhaps most importantly, how key learnings will make the system better through adaptation!

a. Should government consider a single reporting portal for all cyber incidents, harmonizing existing requirements to report separately to multiple regulators?

No. There are privacy, national security, and the potential creation of new risks with a single portal. Need to know principles coupled with anonymized data practices should be a start. Work with the Cybersecurity Expert Group and International Advisory Board to develop adaptive standards.

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

Really complex question. There are first discussions on Root-Cause (RCA – Root Cause Analysis), then impact assessment, security standard compliance and readiness assessment, crisis response effectiveness and key learnings, risk acceptance and risk model checking, …and so on. The Cybersecurity Expert Group and International Advisory Board can help with this.

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

There are many different ways. See how recommendations in See Section/Principle #1, Section/Principle #2, Section/Principle #3, Section/Principle #4, and Section/Principle #5 interact to drive comprehensiveness, consistency, and continuous improvement to the processes.

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

Guidance, frameworks that fit their needs, low cost solutions/best-practices, easy risk assessment tools, temp/interns for security projects, mentorship, and incentives/subsidies if possible.

16. What opportunities are available for government to enhance Australia's cyber security

technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Expert guidance to identify the best types of tools (Cybersecurity Expert Group, Sector Experts, and International Advisory Board can help). Innovation incubation support for cutting-edge security tools. See Section/Principle #3 Risk Controls for more recommendations.

17. How should we approach future proofing for cyber security technologies out to 2030?

Strategic planning from experts that have proven track records of predicting the shifts in the industry, including the threats. Build a strategy that is adaptable and sustainable from the best expert pool possible. See Section/Principle #1 for more thought leadership recommendations.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

Yes! Government spending is a huge incentive which can establish standards and expectations further downstream and into non-government supplier domains. It must be done with foresight because if the cost or friction associated with the expectations are too high, it can be an inhibitor to innovation and investment. See sections Section/Principle #1, Section/Principle #2, Section/Principle #3, and Section/Principle #5 for more recommendations that interlock to enable a healthy advantage.

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

Understanding the future is crucial, both in technology and in how cyber Threat Agents will shift. The attackers maintain the initiative in the cybersecurity industry. Security responds to their attacks. So, knowing them is key to identifying valuable emerging tech.

(Cybersecurity Expert Group, Sector Experts, and International Advisory Board can help)

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

A cybersecurity measures and metrics program must be developed. (Cybersecurity Expert Group, Sector Experts, and International Advisory Board can help).

Reference:

1.12. Establish a centralized cybersecurity metrics reporting and aggregation group for each critical sector to identify trends, issues, and best practices that will disseminate key findings to that sector and the centralized auditing or intelligence group

2.10. Regulations requiring compliance to cross-national agreements and cooperation for sector standards, criminal investigations, real-time threat data, risky product bans/embargos, and metrics information sharing

5.2. Establishing a cybersecurity risk metrics dashboard

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

Leadership and communication/advocacy/evangelism are key. Basically, you need something good to say, know how to say it in a way everyday people understand, then explain the relevance of the message. Not an easy task.

In addition to the Leadership section (Principle #1), also look at these reference in Section/Principle #5

5.5. Establish a national civic education campaign to promote a culture of savvy cybersecurity by communicating:

5.5.1. The relevance of security, privacy, ethics, and safety for digital systems

5.5.2. The best practices that every Australian can benefit from, to improve behaviors

5.8. Promote public/private partnerships that establish long-term improvement capabilities (standards, consortiums, collaborations, etc.)

5.9. Maintain visibility to the public, senior levels of government, and international partners through social media, marketing, and evangelists

5.14. Establish a national public training campaign to communicate the importance of cybersecurity, improve users' behaviors, draw interest into STEM/Cybersecurity jobs, and promote the pursuit of those conducting attacks

5.15. Establish a political body to promote international cooperation for cybersecurity, cybercrime prosecution, community outreach/education, and international protection standards