AIHS Australian Institute of Health & Safety

Submission to the National Cyber Security Strategy 2023-30 Consultation

15 April 2023

Introduction

Founded in 1948, the Australian Institute of Health and Safety (AIHS) is Australia's largest peak body for generalist work health and safety (WHS) practitioners and professionals. Our vision is "safe and healthy people in productive workplaces and communities" (see www.aihs.org.au). We have a long and proud history of working with WHS regulators, employers, unions, and governments in the pursuit of more effective WHS policy, regulation, and practice. We have more than 4,000 members across Australia, and Branch Committees in every state and territory.

Background

We see achieving positive WHS outcomes as being aligned with, and arguably foundational to, Australia's national interests. This is primarily through two lens; 1) safer and healthier workplaces enhance our international competitiveness by attracting and retaining international talent, both skilled and unskilled, and 2) we know that safer and healthier organisations, both public and private, are more likely to be more efficient and effective in achieving their business objectives. Positive WHS outcomes are at the heart of achieving improved productivity.

As the Discussion Paper notes, the changing nature of work, not the least of which through the rapid COVID-19-driven increase in hybrid and remote working arrangements, has increased some WHS risks significantly. Our position is that cyber events can and do have WHS impacts, on workers, employers or persons conducting a business or undertaking (PCBUs), and third parties such as customers. These impacts are often psychological in nature, such as anxiety, stress, and other forms of poor mental health. And these impacts can be and are physical, such as reactions linked to psychological impacts, and in some cases direct risks to physical safety.

Whilst these impacts may not occur in the traditional construct of WHS harm (e.g. PCBU activities leading or tangibly contributing to worker/s sustaining an injury), we note for the benefit of the Expert Advisory Board that Directors of corporations, as Officers under model WHS legislation which is in effect in most jurisdictions, have duties and due diligence obligations under section 27 (see Model laws at https://www.safeworkaustralia.gov.au/law-and-regulation/model-whs-laws).

These obligations include gaining an understanding of the nature of the business' operations and hazards and risks associated with those operations, and ensuring that key stakeholders have the relevant resources, processes, and training to discharge their obligations in relation to WHS hazard and risks. Our view is that Directors (and all Officers as defined by the Model legislation) should have cyber security risks on their risk registers or equivalent management system, and that the potential WHS impacts of these risks should be understood and accounted for. As more and more work is done through cyber means and in cyber spaces, we believe Directors and Officers should take a holistic view to the impacts of cyber risks and harms.

Further, WHS duty-holders are also obligated to eliminate/mitigate WHS risks to third parties affected by the activities of their business. Depending on specific circumstances, cyber incidents and their associated psychological and/or physical harm could be interpreted as applicable to this framework. Whilst we are unaware of any case law demonstrating this line, we anticipate that, given the convergence of several key trends (e.g. cyber-based work, psychological harm, rates of cyber incidents), a seminal case is likely to occur soon.

We note that the 'Our partners' section of the Department of Home Affairs cyber security website lists the eSafety Commissioner (see www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/our-partners). And examples of "online harms" include "exploitation of vulnerable people, online bullying, and illegal or harmful content". These stakeholders and themes have strong connections and overlap with WHS issues, risks, and harms.

In relation to psychological health and safety, we note that since the previous 2020 Cyber Security Strategy was implemented, multiple jurisdictions have legislated psychological health and safety-specific regulations and codes of practice into their WHS legislative frameworks. Amplified by the Respect at Work initiative and others (see https://www.respectatwork.gov.au/), psychological health and safety is growing rapidly in prominence as a WHS issue across the country. Digital technologies and cyber means are often an enabler and/or contributor to workers and other parties experiencing psychological harm.

To that end, we recommend the country's nine general industry WHS regulators (listed at https://www.safeworkaustralia.gov.au/law-and-regulation/whs-regulators-and-workers-compensation-authorities-contact-information by the national WHS policy body Safe Work Australia) should be added to this list of stakeholders as the entities primarily responsible for regulating WHS in Australian workplaces. Safe Work Australia may be an ideal intermediary for these bodies.

Key messages

Don't forget the WHS legislative framework and broader WHS ecosystem

We note that the *Quad Cybersecurity Partnership: Joint Principles* explicitly states that the incapacitation or destruction of critical infrastructure sectors would impact national public health and safety (see section 4 in https://www.homeaffairs.gov.au/cyber-security-subsite/files/qscg-joint-principles.pdf); our view is this also encompasses work health and safety.

By incorporating cyber risks and harm into the WHS ecosystem, stakeholders can leverage the mature, established WHS framework to support risk mitigation and harm reduction in relation to this newer field of cyber. This means integration at the individual, organisation, and regulator levels.

Whilst some (particularly legal) views assert that the WHS legislative framework is evolving into a 'legislation of last resort', as issues such as discrimination and sexual harassment are brought into the framework, we propose that this trend is because the WHS framework is conceptually robust, and operationally sound. An example of this in Victoria is the recently updated environmental regulatory framework, which adopts very similar legal concepts (e.g. general environmental duties, duty holders etc.) and terminology to the Victorian occupational health and safety legislative framework.

The WHS aspects of cyber harm must not be overlooked

More Australians are working through cyber means than ever before, and this trend will increase. We ask that the Expert Advisory Board when developing their recommendations for the 2023-30 Strategy do not omit the WHS context, frameworks, and impacts that cyber risks, incidents, and harms can present.

We endorse and highlight the prominence WHS receives in the 'Back to Business' November 2021 briefing (see pg. 4 of https://www.homeaffairs.gov.au/cyber-security-subsite/files/back-to-business-hybrid-workforce.pdf).

Responses to Discussion Paper questions

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

We believe that WHS should be included throughout and considered to be a fundamental component of the new Strategy. In particular, reference should be made to Australia achieving and maintaining international competitive advantage through the provision of healthy and safe workplaces, including those involving cyber work, and the value proposition this provides to attract and retain international talent.

We question how one would begin to assess whether we achieve being 'the *most* cyber secure nation in the world', and the value this primacy entails. For example, how would this vision be measured and compared with the status of other nations? But we support the longer-term ambition of the Discussion Paper.

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

We note for the Expert Advisory Board's benefit that Australia already has a WHS legislative and regulatory framework across nine jurisdictions (the eight states and territories and the Commonwealth). Safe Work Australia also administers the 'model legislation', which most of the jurisdictions seek to replicate.

As part of the new Strategy, the Board may consider investigating whether cyber-related risks, incidents, and harms are explicitly covered by WHS model legislation. This would require consultation with Safe Work Australia and their tripartite constituents. This action would obviously require more detailed forecasting and substantiating to warrant any regulatory amendments.

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)?

No comments.

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?

No comments.

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

As alluded to above, we would support further work being done in this area, with the WHS context being explicitly considered.

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

No comments.

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?

As supporters of growth in productivity in Australian businesses, we support the concept of closely monitoring regulatory burden. Whilst extensive consultation would be required with WHS stakeholders, we propose that the Board consider mirroring or incorporating aspects of a cyber legislative framework into the various existing WHS frameworks. Industry already understand much of these frameworks, in terms of design, concepts, and processes (e.g. notifiable incidents).

f) Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:
   a) victims of cybercrime; and/or
   b) insurers? If so, under what circumstances?
      i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

No comments.

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

No comments.

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

At the AIHS we consider ourselves to be fortunate to work in a wealthy, developed economy, in a liberal democratic society. Whilst there is still much to be done in Australian WHS practices, regulations, and outcomes, we know that we are in a privileged situation where most workplaces are comparatively healthy and safe, PCBUs and workers are supported and regulated by robust justice systems, and standards of healthcare and environmental practices are high. This is not the case for all of our nearest international neighbours.

We believe that this updated Strategy should adopt a generous, conciliatory approach to our regional partners. By exporting and sharing our technical and professional capabilities, the broader region stands to benefit from higher standards of practice, shared understanding, and ultimately improved outcomes. In this sense there are many similarities between cyber security and WHS.

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

As Australia's largest peak body, we advocate for WHS professionals on WHS matters to advance our members' interests and improve Australian WHS outcomes. But we also play a role internationally; we are active participants and contributors within the International Network of Safety and Health Professional Organisations (INSHPO) (see www.inshpo.org/work).

Our role within this framework enables engagement and dialogue with international peers from a diverse range of nations. Of the four Quad Leaders, we note that the American Safety Society of Professionals (ASSP) and Board of Certified Safety Professionals (BCSP) represent the United States of America. India and Japan currently do not have representatives within the INSHPO framework.

Separately, the Japan Industrial Safety and Health Association (JISHA, https://www.jniosh.johas.go.jp/en/) is the preeminent equivalent body in Japan, and the National Safety Council of India (NSCI, https://nsc.org.in/) is the equivalent body in India. AIHS personnel have more informal connections and relationships (i.e. outside of formalised structures and frameworks) with these stakeholders.

We note that whilst the 2020 Strategy included dollar commitments to international partnerships, to build confidence and provide certainty we would expect to see more details on how proposed budgets would be spent, such as the high level objectives, responsibilities, and timelines funding recipients would hold.

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 behaviour in cyber space?

A key function we perform is coordinating the appointment of Australian-based WHS professionals and experts on to international standards committees. Our focus is on WHS and related standards. We would be happy to share our views directly in confidence with the Board consultation team on the effectiveness and challenges in the processes through which international standards are developed.

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

No comments.

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

No comments.

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 organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

For the benefit of the Expert Advisory Board, we note that the one of the greatest inherent challenges faced by all WHS regulators around Australia is their dual role; that of 1) educating and supporting the business community and others regarding WHS advice and information, and public communication and behavioural influencing campaigns, and 2) implementing compliance and enforcement programs, including on-site inspectorate activities, which can lead to legal cases being brought in courts. This inherent conflict of roles can make it challenging for regulators to gain the trust of stakeholders. These tensions/challenges must be addressed in the cyber equivalent reporting scheme.

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?

For the benefit of the Expert Advisory Board, we note that regulators and other government and statutory entities need be mindful of incident notification framework design. A recent example of arguably poorly designed frameworks or policy was when positive COVID-19 cases were required to be notified to WorkSafe Victoria during the pandemic. Cases then significantly increased, rendering the process a high administrative burden on duty holders (e.g. employers), for widely perceived very little value in return (e.g. insights or even basic reports coming back from the regulator). This unexpectantly high volume also meant the regulator could not respond in any meaningful way to individual reports.

We share this example as a case study in the need for caution in designing/considering mandatory reporting policy. Particularly in a rapidly changing cyber threat environment, mandatory reporting may lead to unintended consequences, such as high administrative/resource burden from reporters and report-receivers, public desensitisation (e.g. COVID-19 case numbers ‘losing meaning’ through the pandemic), and other inadvertent effects.

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

No comments.

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

No comments.

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

Many more Australians are working from home now compared to 2019. To this end, in 2020 we developed *Workers Working from Home* chapter of a free resource we auspice called the Occupational Health and Safety Body of Knowledge (see https://www.ohsbok.org.au/2231-2/). More initiatives like this are required to support workforces to build both their understanding of WHS at home, and their cyber safety at home. We would welcome the opportunity to collaborate with the Department of Home Affairs and other interested stakeholders to develop further guidance and resources for industry and workers that focuses on this cyber-WHS nexus. We believe this would assist in getting cyber safety messaging and information to other audiences.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?
    a) Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

No comments.

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

No comments.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?
    a) What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

As in WHS, smaller businesses experience proportionally greater rates of harm, largely due to less access to supporting resources and expertise (either inhouse or external). We propose the Board look to the WHS system, such as WorkSafe Victoria's OHS Essentials Program (see https://www.worksafe.vic.gov.au/ohs-essentials-program), for examples of how government can support smaller businesses in meaningful ways. This approach requires well designed participant screening/vetting processes (e.g. cyber consultants must meet minimum capability and practice standards).

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?

No comments.

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

No comments.

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?

No comments.

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

Safety in design is a core and important component of effective WHS practice, regulation, and outcomes. Good design is incredibly powerful in mitigating or eliminating downstream risks from materialising and harming people. But linking design, including the system parameters and decisions from designers, with outcomes, which are often temporally and geographically dispersed, is very difficult in complex systems. For this reason, WHS regulators have struggled to regulate and enforce design-related duties. Compliance and enforcement will therefore likely also be challenging in relation to cyber design. Design standards must therefore rely more on strong industry promotion and education. Government should think about what examples of poor security by design might look like, and what the consequences are, in order to demonstrate to industry stakeholders what is and isn't acceptable.

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

We would expect 'theory of change' and 'impact measurement' techniques to be used to design a measurement framework that not only collates cyber incident data, but also is sophisticated enough to measure successfully deterred attacks. Like WHS, cyber environments are complex systems. Any efforts to measure should therefore be multi-faceted. This may mean including metrics such as periodic population or other audience surveys, measuring awareness, state of knowledge, and performance of defined actions.

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

No comments.

We appreciate the opportunity to provide input into this consultation. We trust that our submission provides the Board and other stakeholders with perspectives which, being from outside of the cyber domain, are unexpected but worth considering.

Kind regards,

Andrew Heinrichs

Chair, AIHS Policy Committee