Submission to the National Cybersecurity Strategy Discussion Paper

Submitter: Cybermindz.org Ltd

1 Executive Summary

A nation that is cyber-defenceless due to burnout and low morale of cyber defence teams is an easy target. There is an urgent need to harden our human cyber defences in preparation for a possible escalation in cyber conflict, including attacks on supply chains, critical services and infrastructure. In practical terms, this translates to optimising mental resilience in our cyber professionals.

Quantitative research is showing a degradation in the mental health of cyber teams, with loss of skills now underway or predicted. Anecdotal evidence also suggests new entrants into cyber may lack resilience to prevent a progression into burnout.

Fortunately, direct, peer-informed, evidence-based and scalable mental health support is now available to cyber teams to reverse this trend with restorative and preventative programs. Cybermindz.org is an Australian-founded, not-for-profit which is pioneering in this space using a mental health support protocol with extensive prior and current military application.

The Cybermindz initiative has received early Australian State government and private sector recognition and support. This recognition and support needs to now be taken up by the Federal Government, and mental health in cybersecurity formally acknowledged as a critical component of our national cybersecurity strategy.

2 Introduction

Cybermindz.org is an Australian not-for-profit dedicated to promoting cybersecurity mental health awareness, providing direct and scalable preventative and restorative interventions in cybersecurity professionals through measurable, evidence-based programs.

Through this lens, and from our consultations with many in the industry, we are pleased to offer our insights on the National Cybersecurity Strategy Discussion Paper.

3 About the organisation

Cybermindz' founder, internationally respected internet and cybersecurity industry leader, Peter Coroneos began piloting mental health support programs with members of the Cybersecurity Advisors Network in 2021 and started seeing positive changes within a relatively short time. This inspired him to formally constitute a not-for-profit social enterprise dedicated to bringing the protocol to the greatest number of cyber workers possible.

Patron

Cybermindz' Patron is retired High Court Justice, The Hon. Michael Kirby AC, CMG.

Founding partners

- Deloitte
- NSW Government
- CyberCX
- Mimecast.

Formal cooperation MoUs or endorsements are in place with

- AISA (Australian Information Security Association)
- CAUDIT (Council of Australian Universities Directors of IT)
- CI-ISAC (Critical Infrastructure ISAC)
- Cybersecurity Advisors Network.

Board and leadership

The Cybermindz board includes Peter Coroneos, leading cybersecurity research psychologist, Dr Andrew Reeves, Lt Col (ret'd) Richard Mogg and iRest Australasia Director, Fuyuko Toyota. Collectively, they provide the organisation with strong leadership, a clear focus, strong expertise in the protocol and its delivery and a depth of experience across domains. Respected CISO, Kevin Shaw leads the organisation's ambassador program which is attracting high profile cyber leaders as advocates.

Pilot programs completed or in progress

Cybermindz has completed, is running or is shortly to commence pilot programs with cyber teams from CyberCX, Allianz Insurance, NSW Government, Monash University, Department of Defence and the Australian Signals Directorate. It is also in rollout discussions with two other state governments.

International expansion

On April 24, the organisation will launch in the US with the support of CISA Director, Jen Easterly and a number of high profile cybersecurity leaders. It will hold the inaugural "Mental Health in Cybersecurity Leadership Summit" in San Francisco coinciding with RSA Conference. See her call to action on our behalf in the short video at the end of this submission. Further establishment in other 'Five-Eyes' jurisdictions is in planning.

4 Our Response to the Discussion Paper

Respectfully, we find it striking that the Discussion Paper is devoid of recognition of the mental health challenges facing cyber teams.

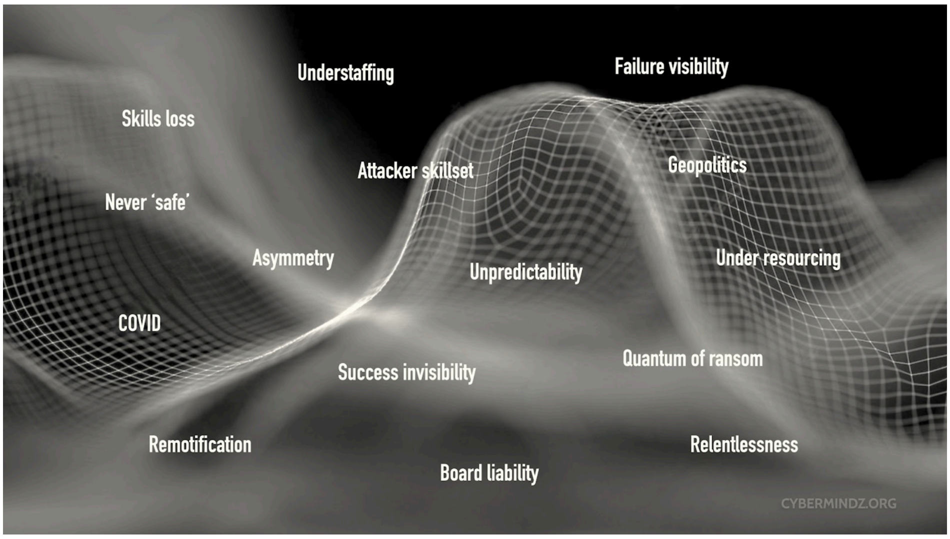
Burnout is endemic in the cybersecurity industry, there is hardly a CISO forum these days where it is not discussed. There is almost universal consensus within the sector that this is a critical issue that must be addressed.

Yet there is not a single reference to it, nor even a hint of the relationship between the psychological challenges of the profession and our national cyber resilience or Australia's national cyber skills strategy. Nor of its potential downstream consequences if left unaddressed.

The nature of the work in cybersecurity is highly demanding, and the stakes are incredibly high. Cybersecurity professionals are constantly battling sophisticated adversaries who are trying to steal sensitive data, disrupt critical infrastructure, and undermine national security. These professionals must also keep up with the rapidly evolving threat landscape and stay up to date with the latest technologies and best practices.

These demands can take a significant toll on the mental health and wellbeing of cybersecurity professionals. Our research has shown that burnout is common among cybersecurity professionals. The highly demanding nature of the work, coupled with long hours and tight deadlines, often creates a stressful and pressure-filled work environment.

Additionally, the ever-increasing volume of alerts, incidents, and false positives can create a sense of overwhelm and helplessness, leading to feelings of burnout. The following schematic shows the unique combination of 15 factors that come to bear on cyber teams.



The quote below from a respected military academic puts in context the relationship between human dimension of cyber operations and the threat environment.

> "[Our main geopolitical adversary] deploys a comprehensive capability to engage in protracted offensive cyber operations against its adversaries. Hence, it can attack Australia by means of a sophisticated cyber offensive campaign, even without a formal declaration of hostile intent.
>
> … [they] can regularise and intensify cyber-attacks on Australian key assets to cause more disruption and inflict more damage.
>
> … more action is possible now. For example, the ADF can ensure command superiority by protecting its own communications, command, control, computers, intelligence and interoperability (C2I4) structures, systems and networks from hostile disruptive operations, while denying an adversary the ability to utilise theirs. It can also enhance *the moral readiness and the determination of troops to fight and win under any circumstances, including unfavourable battle conditions.* [emphasis added]
>
> *Dr Alexey Muraviev, Australian Defence Review, 2 September 2021*

This analysis applies equally to the private sector whose cyber defenders are under pressure defending our national services and infrastructure.

The recent attacks on Medibank, Optus and Latitude Finance demonstrate the effect on public confidence when adversaries succeed. It is not difficult to anticipate that a committed adversary could have a catastrophic effect on national morale were it to institute a concerted attack against multiple services both in public and private control.

The government has legislated to hold infrastructure providers more accountable for their level of exposure to cyber risk and to strengthen sanctions for privacy breaches. Yet we fear a perverse effect, an unintended consequence which we've not seen ventilated elsewhere.

The more boards come into the firing line, the more pressure is ultimately imposed on cyber teams. From a policy standpoint, one priority - making companies care more about cyber - is driving cyber teams into faster decline, undermining another priority - improving national resilience. The answer is not to back away from regulation, but rather to counter this effect by educating boards on the need to nurture, not blame their frontline cyber defenders, for everyone's sake.

It is therefore paramount that we start fortifying the mental resilience of our cyber defenders in preparation for any such future conflict.

5 What our research is showing

Our research indicates that burnout is a significant concern among cybersecurity professionals. In 2022, Cybermindz began a pioneering program of research assessing employee burnout of employees in cybersecurity organisations. Our representative sample of over 110 cybersecurity professionals across 11 organisations provides an accurate snapshot of mental health status in the Australian cybersecurity sector.

Our participants represent a broad range of cybersecurity-specific roles, including CISOs, CIOs, security analysts, penetration testers and security engineers.

We assessed our participants using the Maslach Burnout Inventory (MBI) which defines Burnout as a state of **Emotional Exhaustion** (feeling overwhelmed), **Cynicism** (feeling unmotivated), and **Low Professional Efficacy** (feeling inadequate) caused by excessive and prolonged stress. Burnout occurs when employees feel overwhelmed, emotionally drained, and unable to meet constant demands.

As the stress continues, employees begin to lose the interest and motivation that led them to take on a certain role in the first place. Burnout reduces productivity and saps energy, leaving employees feeling increasingly cynical and resentful. Eventually, they may feel like they have nothing more to give.

Our findings indicate that burnout is a significant concern among cybersecurity professionals. The average score for **emotional exhaustion** was 3.5, which falls within the high range when compared to the Australian general population (high range is >3). The middle 50% of respondents in cybersecurity roles scored in the 2-4.5 range.

A moderate to high range of **cynicism** was also observed, with an average score of 11 (moderate: 6-12) and middle 50% scores ranging from 7-15. The maximum recorded score was 30, indicating an extremely high level of cynicism.

Personal accomplishment scores were moderate to high (high is bad), with an average score of 26 (high range is 27+) and the middle 50% ranging from 21-30. These exceed comparable measures for other groups.

Alarmingly, cyber workers appear to be burning out faster than frontline health care workers. This single metric is a reliable predictor of resignation intent.

Addressing burnout requires a multifaceted approach that prioritises employee well-being and mitigates the negative impacts of burnout on mental and physical health, job performance, and organisational outcomes.

It is not only resignation intent that is foreshadowed. Left unaddressed, the three components of burnout (emotional exhaustion, cynicism, and low professional efficacy) are also strong predictors of:

- Fewer extra-role behaviours (‘going the extra mile’)
- Insider threat (a desire to undermine organisational goals); and
- Lower productivity.

6 Mental Health as Factor in Skills Retention and Attraction

The consequences of burnout for organisational and national security cannot be overstated. In addition to decreased job performance, burnout can lead to errors in judgment, and diminished attention to detail, which can increase the likelihood of successful cyber attacks.

Moreover, when individuals leave the cybersecurity profession due to burnout, it leads to a talent drain that can take years to replenish. This talent drain can leave organisations and even nations vulnerable to cyber attacks and undermine national security.

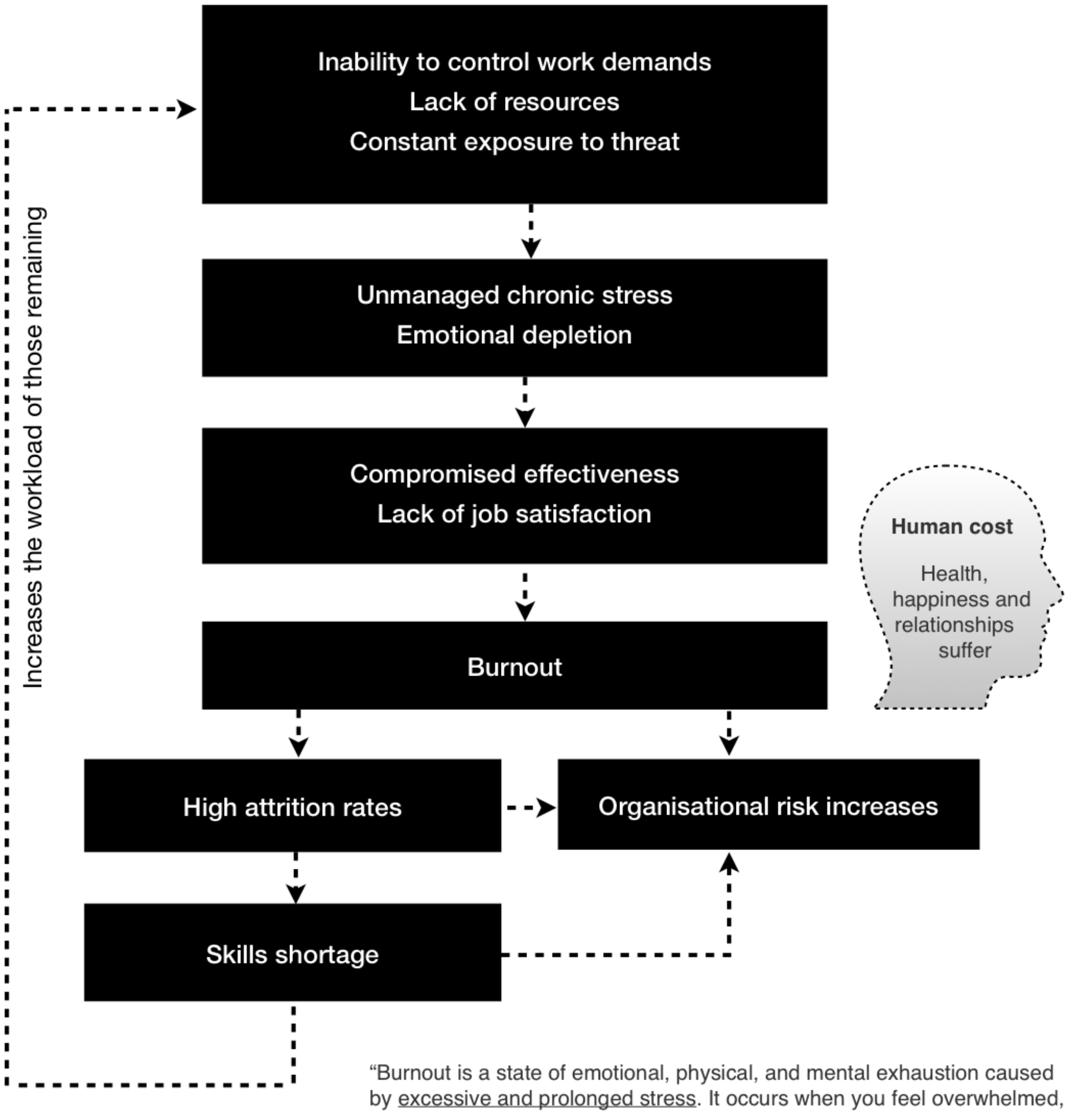
Were cybersecurity as a profession to receive a widespread negative perception about the levels of stress its practitioners face every day, this would deter new entrants and frustrate government and private sector efforts to build this workforce.

Anecdotal evidence suggests that students are opting away from entering the profession because they are aware of the stress levels. This trend is alarming and highlights the urgent need to address burnout in the cybersecurity industry.

There is an opportunity here to reframe the problem into an opportunity. Organisations who wish to attract good talent, who prioritise the wellbeing of their cybersecurity professionals and implement strategies to prevent and manage burnout will have an advantage in attesting talent. In a competitive skills market a culture which supports wellbeing will be a factor in the choice of employer.

For government employers who cannot generally match private sector salaries, wellbeing initiatives as well as other workplace incentives like flexible working arrangements can serve as a buffer against skills loss.

An Impending Cybersecurity Skills and Capability Crisis?


Inability to control work demands
Lack of resources
Constant exposure to threat
Unmanaged chronic stress
Emotional depletion
Compromised effectiveness
Lack of job satisfaction
Burnout
Human cost
Health, happiness and relationships suffer
High attrition rates
Organisational risk increases
Skills shortage
Increases the workload of those remaining

> “Burnout is a state of emotional, physical, and mental exhaustion caused by excessive and prolonged stress. It occurs when you feel overwhelmed, emotionally drained, and unable to meet constant demands. As the stress continues, you begin to lose the interest and motivation that led you to take on a certain role in the first place.
>
> Burnout reduces productivity and saps your energy, leaving you feeling increasingly helpless, hopeless, cynical, and resentful. Eventually, you may feel like you have nothing more to give.
>
> The negative effects of burnout spill over into every area of life—including your home, work, and social life. Burnout can also cause long-term changes to your body that make you vulnerable to illnesses... Because of its many consequences, it’s important to deal with burnout right away.”

Source helpguide.org

It is essential to emphasise that skills retention of the highest value skills, such as Chief Information Security Officers (CISOs), are most at risk from burnout. These are individuals with 10+ years of experience who carry the corporate memory and may be difficult to replace. Losing such highly skilled individuals can have a significant impact on an organisation's ability to manage cyber risks effectively.

We also see an acute situation in Security Operations Centre (SOC) analysts who face a daily barrage of alerts, which they have to evaluate and triage. A single error can have devastating downstream consequences. They know this and carry that burden. Their hyper-activated brains develop an inability to switch off. The neuroscience suggests this may due to neuroplastic effects governing a person's internal 'locus of control' arising from elevated levels of cortisol, among other drivers.

However, burnout extends beyond those classes, into incident responders, governance risk and compliance (GRC) teams, and others engaged in cyber defence and response capacities, or areas whose functions are impacted by breaches.

Two scenarios are foreseeable. The cascading and mass consequential effects in an organisation and arguably large sections of the population of a single failure in a cyber team. Or a depleted cyber team's incapacity to prevent an attack caused by negligence in another part of the organisation. Either should convince policy makers that this is a cohort warranting special focus and support.

7 About Cybermindz' Approach and Capability using the iRest Protocol

Cybermindz' current delivery platform places central importance on the iRest (or Integrative Restoration) protocol. iRest is an evidence-based mind-body protocol for optimal health, healing and well-being, which can be delivered remotely or in person, individually and in groups.

Within Australia there are over 400 trained iRest instructors (7000 worldwide) including two of the present authors of this submission, Peter Coroneos and Richard Mogg.

iRest was developed by clinical psychologist Dr Richard Miller as the result of over 40 years of research. The first formal study of iRest took place in 2006 at Walter Reed Army Medical Center (WRAMC) in Maryland, USA, to assess its feasibility as a potential adjunct treatment for PTSD among active-duty soldiers returning from the Middle East.

Participants reported less reactivity to situations beyond their control, increased calm and being more able to enjoy life. The results launched an ongoing program of iRest classes across the U.S. military. The iRest protocol has be used successfully by the U.S. Military since 2004 to manage and prevent stress, burnout and trauma.

There have been over 30 studies conducted into the efficacy of iRest. It is used at over 85 military bases across the U.S, Canada and Europe as well by deployed military personnel. In 2010 the U.S. Army surgeon General endorsed iRest as an approved Tier-1 complementary treatment.

iRest has delivered positive results in the Australian Defence Force and by Australian veterans organisations since 2016, including at Soldier Recovery Centres. It has also been applied in resilience, wellbeing and human performance programs delivered to the Australian Army, Special Forces and Air Force.

How iRest works

iRest is a ten-step guided practice. It combines modern understandings of psychology and neuroscience, adapted for both clinical and non-clinical application. It incorporates physiological and psychological principles from other forms of therapy, including cognitive-behavioural therapy (CBT), autogenic suggestion, progressive muscle relaxation, Jungian and Gestalt psychology and Eye Movement Desensitisation and Reprocessing (EMDR) and exposure therapy. It is trauma-aware and can be practised safely by anyone, regardless of physical ability or experience. Since it is a guided practice, there is no need to learn a technique. Benefits are generally felt immediately.

Over several weeks, iRest also functions as a neural training regimen, targeting core body, mind, and brain skills and functions that are important for wellbeing, resilience and success in daily life. It enhances brain function in the areas of sensory, motor, and limbic and the prefrontal cortex.

Its application reshapes neural pathways critical to fostering emotional self-regulation, ethical decision-making, resilience, enhancement of cognitive and emotional skills, development of empathy, well-being and optimal performance. Research indicates that it effectively builds mental and physical resilience, alleviates anxiety, insomnia, chronic pain, depression, post-traumatic-stress-disorder (PTSD), enhances general well-being and promotes optimal human performance.

From these initial beginnings with the military, the application of iRest has been extended to diverse populations including community centres, chemical dependency units, homeless shelters, schools, hospices and palliative care facilities, correctional facilities and applied to traumatic brain injury, chronic pain, multiple sclerosis, fibromyalgia, anxiety, compromised nervous systems or trauma, chronic pain, sleep disorders and chronically high stress levels.

8 Application of the iRest protocol into cybersecurity

With the backing and support of the founder Dr Richard Miller and his iRest Institute, Cybermindz was authorised to develop cyber-specific scripts of delivery of the protocol. This is the first application of the protocol into cyber anywhere in the world. We have considered the specific challenges faced by cyber security professionals and have adapted the protocol to meet the specific needs of cyber security professionals.

Our programs have received a high degree of acceptance in our pilot programs because they are perceived as having been developed from within the sector by people who understand directly the unique factors challenging the mental health of cyber teams.

Our challenge like many, not-for-profits is having the resources to make the greatest impact in the shortest possible time. To that end, we urge the Federal Government to consider how it may support our work as a matter of priority.

9 Recommendations

A. That the Review Committee include reference to the mental health dimension of cybersecurity and call for action and resourcing of efforts to build psychological resilience in our core defenders.

B. That the Government elevate mental health support of cyber teams as a national security strategic priority, along with building sovereign capability in critical systems and processes.

C. That the Government support research efforts to track over time the baseline status of mental health in cyber teams.

D. That the Government allocate funding to accelerate the capability, delivery and rollout of expanded mental health services to cyber teams in both the pubic and private spheres. These services should be cyber specific, evidence based, military proven, measurable and peer informed.

E. That the Government support efforts to build mental resilience into new entrants into cyber profession as a preventive measure against burnout and for the promotion of sustainable levels of human performance in these critical workers.

F. If the Government agrees with our perspectives, we would seek its assistance to expand our programs through the Five-Eyes nations, as the former Rudd

Government did with *icode* in 2010, which later saw adoption of a parallel program in the US covering nearly 300 million internet users.

10 Conclusion

In conclusion, Cybermindz.org urges the National Cybersecurity Strategy to recognise the mental health dimension in cyber teams and prioritise efforts to address burnout. The cybersecurity industry is critical to national security and must attract and retain the best talent. Failure to address burnout will have significant consequences for the cybersecurity industry and national security.

We stand ready to support the efforts of the National Cybersecurity Strategy to address this issue and promote a healthy and sustainable cybersecurity workforce.

For and on behalf of Cybermindz.org Ltd
Peter Coroneos, Executive Chairman
Dr Andrew Reeves, Director of Organisational and Behavioural Research
Lt. Col. (ret'd) Richard Mogg, Executive Director

12 April, 2023

* Watch this one minute video from US Director of CISA, Jen Easterly offering words of support for our Australian-founded cyber mental health initiative as we prepare to enter the US as part of our international rollout in 2023.