Mental Health

in the Australian Cyber Security Industry

A survey of cyber security professionals conducted by

sekuro

A note from **Noel Allnutt**, Managing Director of Sekuro

"Long hours, mounting pressure, a to-do list that never seems to end: this is what we talk about when we talk about burnout at work.

"Chances are everyone has experienced it at some point in their lives — I know I certainly have — but my goal is that when my teams experience these feelings, that they are temporary and manageable, with robust support systems and strategies in place to help pull a sufferer out of a damaging headspace.

"Cyber security professionals were faced with unique responsibilities when it came to managing the technological fallouts of pandemics, wars, and accelerated digitisation over the past few years.

"Tasked with an ever evolving series of cyber threats to combat, the industry came under intense scrutiny as high-profile breaches made executive leaders sit up and take notice of the reputational and financial threats posed by cybercrime.

"At Sekuro, we are committed to the mental health of our teams. This October marks Mental Health Awareness Month, and we were keen to shine a light on this issue by surveying professionals from across our industry, to get a sense not only of how the past two years has personally impacted them, but provide a framework for success on how to address some of the challenges we continue to face as an industry when it comes to taking care of ourselves.

"Any leader worth their salt wants their teams to enjoy camaraderie and satisfaction in their work, and thrive professionally in their development and sense of self. For leaders across the industry, I hope these findings help you get an insight into how your team might be feeling so you can start making some proactive improvements this Mental Health Awareness Month."

A note from **Amber Rules**, Clinical Counsellor and Mental Health Educator

"Given the stress and strain of the past few years, it's understandable that many people in the cyber security industry are struggling with burnout and mental health challenges.

"Burnout is the result of ongoing and seemingly unresolvable occupational stress. It impacts many aspects of a person's life, including their mental capacity, effectiveness and energy. It can also cause increased negative emotional experiences such as frustration, anger, overwhelm, negativity and cynicism.

"It can have very real impacts not just on a person's work but also their life outside of the office. This contributes to the wider issue we're seeing play out across the country with increased mental health challenges amongst Australians."

Overview of methodology

Sekuro conducted a survey of 101 cyber security professionals using Zoho Survey from 31 March - 24 August 2022. The survey was shared via Sekuro's LinkedIn account and customer database, as well as its community partners including ISACA Sydney Chapter, Cyber Risk Meetup and MySecurity Marketplace.

The data captures survey answers from 101 participants residing in Australia and overseas at the time of completion of the survey.

Of the 101 participants, 12% were from outside Australia, including Singapore, Japan, the United Kingdom, the United States and Canada.

Key findings

Respondents provided the following insights about their mental health and how it's impacted by their work in cyber security

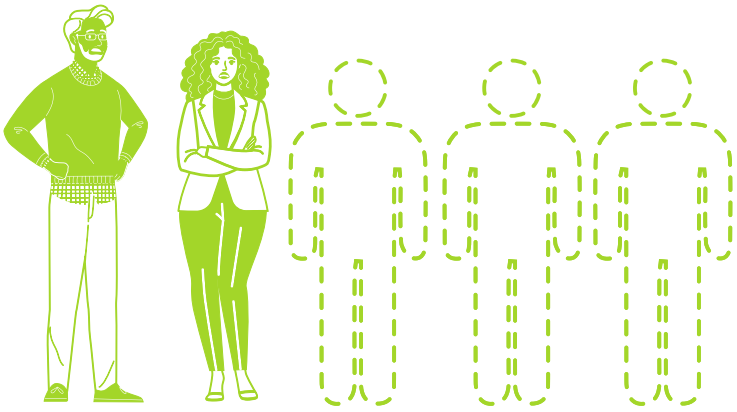
9 in 10 91% of cyber security professionals reported experiencing mental health challenges at work over the past two years

51%

Half of respondents attributed their mental health struggles at work to poor culture and/or management styles

50%

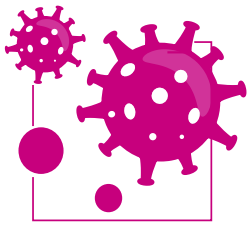
Half said the high-stress nature of a job in cyber security impacted their mental health



Almost 2 in 5

37% quit their jobs in cyber security in response to mental health issues, with 9% changing career paths altogether

Why was 2020–2022 such an intense time for cyber security professionals?



The expansion of the threat landscape

The Australian Cyber Security Centre found that over the 2020-2021 financial year, the COVID-19 pandemic "significantly increased the (cyber) attack surface and generated more opportunities for malicious cyber actors to exploit vulnerable targets in Australia."[1] This culminated in a 13% rise in cybercrime reports from the previous financial year.

Emergence of new threatening actors

Shortly after the Russian invasion of Ukraine, The Australian Cyber Security Centre issued a statement urging Australian organisations to "urgently adopt an enhanced cyber security posture."[2] It claimed the risk of cyber attacks on Australian networks and critical infrastructure was both directly and indirectly heightened after the attack on Ukraine.

The halt to skilled migration exacerbating existing challenges in hiring

The COVID-19 pandemic created yet another headache for the cyber security industry, one that has an obvious correlation with burnout. There's simply not enough cyber security professionals nationally to do the extensive amount of work needed to keep corporations, governments, and individuals safe from cyber crime. AustCyber estimates nearly 17,000 more cyber security workers will be needed by 2026 in Australia[3] — and even this level of growth is not sufficient enough to meet the medium-term shortfall in skills.

1. Australian Cybersecurity Centre, 2021. *ACSC Annual Cyber Threat Report*. [online] Available at: <https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21> [Accessed 29 September 2022].

2. cyber.gov.au. 2022. *2022-02: Australian organisations should urgently adopt an enhanced cyber security posture*. [online] Available at: <https://www.cyber.gov.au/acsc/view-all-content/advisories/2022-02-australian-organisations-should-urgently-adopt-enhanced-cyber-security-posture> [Accessed 29 September 2022].

3. AustCyber, 2022. *Australia's Cyber Security Sector Competitiveness Plan*. [online] Available at: <https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3> [Accessed 29 September 2022].

sekuro

In the survey, Australian cyber security professionals reported *distressingly high levels of mental health challenges*, with only 11% saying they hadn't felt burnt out

Burnout is as an occupational phenomenon rather than a medical condition. However, burnout can still result in very real physical and emotional symptoms.

It can cause increased feelings of negativity, cynicism, avoidance, frustration, anger and overwhelm.

"Burnout is characterised by three dimensions:

- feelings of energy depletion or exhaustion;
- increased mental distance from one's job, or feelings of negativism or cynicism related to one's job; and
- reduced professional efficacy."[4]

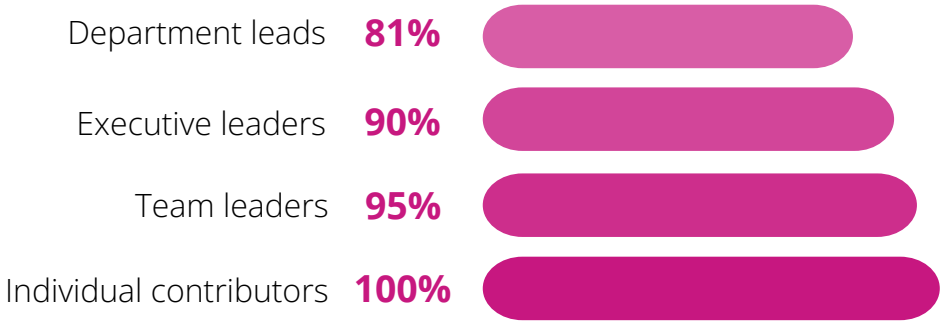
Ways organisations can prevent and manage burnout, according to **Amber**:

- Adopting flexible hiring and work policies
- Making onsite childcare provisions for employees
- Offering flexible leave policies
- Giving bonuses and incentives
- Creating opportunities for meaningful work and special projects
- Creating opportunities for professional development and career progression
- Executive and management immersion programs to develop a robust understanding of workplace wellbeing and practices
- Genuine interest in employee wellbeing
- Employee Access Programs that offer counselling and other mental health supports

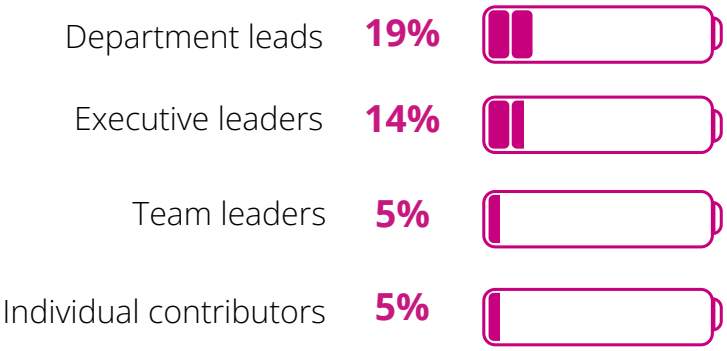
4. World Health Organisation, 2019. Burn-out an "occupational phenomenon": *International Classification of Diseases* [online]. Available at <https://www.who.int/news/item/28-05-2019-burn-out-an-occupational-phenomenon-international-classification-of-diseases> [Accessed: 29 September 2022].

Key statistics indicating the prevalence of mental health challenges

Seniority of those experiencing mental health challenges

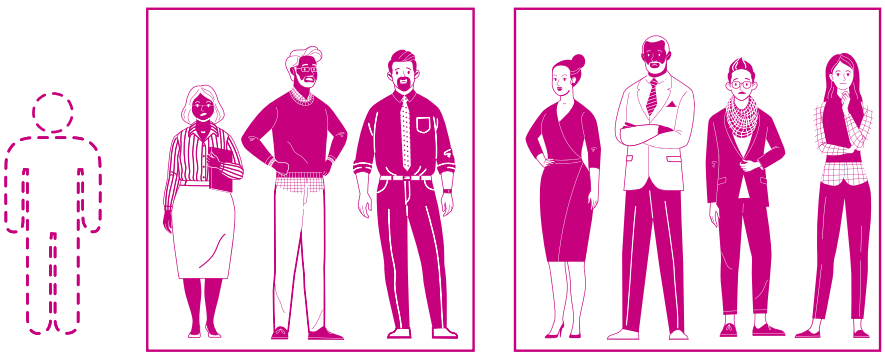


Seniority of those *not* experiencing burnout



How many of your colleagues have been impacted by mental health issues in the past two years?

These results point to a potential lack of openness in particular workspaces when it comes to mental health, given 91% of respondents reported suffering from mental health challenges themselves.



None
18%

Between 1-3
38%

4 or more
42%

sekuro

Top reasons for mental health challenges

When it comes to mental health in the workplace, respondents were asked about their top four contributing factors towards mental health challenges.

51%

Poor culture and/or management styles

50%

The high-stress nature of working in cyber security

41%

My company and/or team is underfunded

37%

There's a lack of required skills in my team and/or company

Dealing with personal uncertainty

Imposter syndrome was a surprising addition to poor mental health outcomes in cyber security professionals. A third of people said imposter syndrome contributed to mental health issues. The inability to believe that personal success has been legitimately achieved or deserved is a concern that permeates many different professional services. This can be attributed to facts such as unrealistic expectations, internalised pressure about factors beyond one's control, or a general lack of empathy from teams about how to address challenges.

In cyber security, this can be attributed to the fact it's possible to climb the corporate ladder quite quickly off talent and opportunity alone, rather than as a result of formal qualifications. The enormous pressure on senior cyber security leaders not to expose their organisations to any vulnerabilities also contributes to a constant undercurrent of failure.

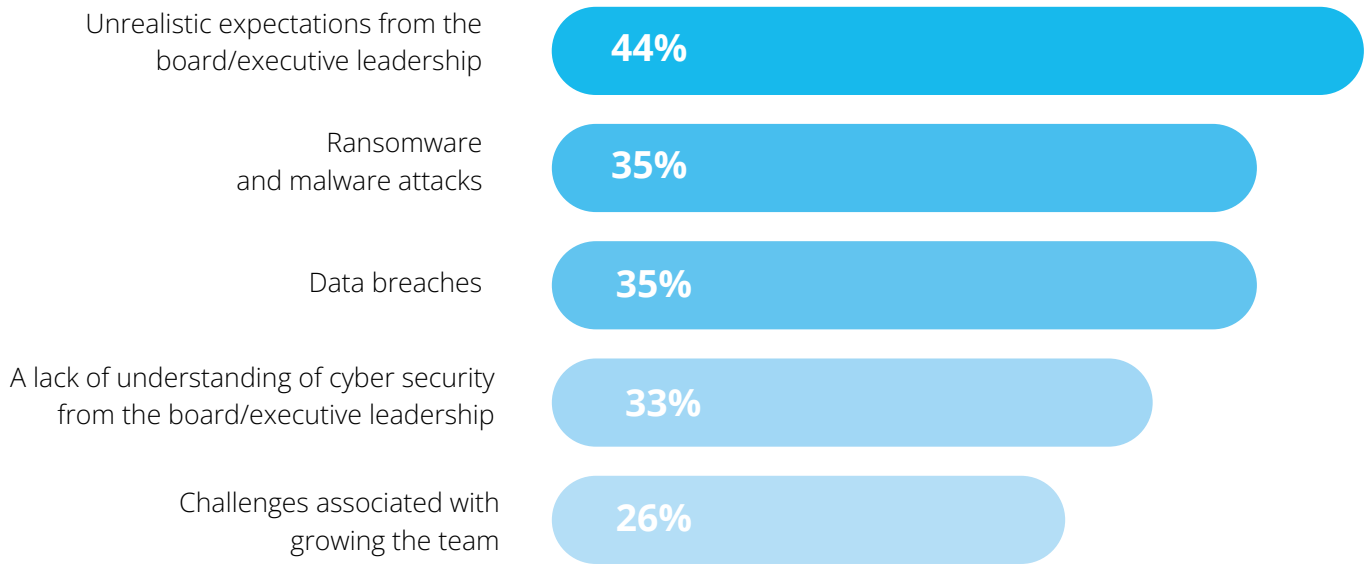
There are proactive ways to reduce the impacts of imposter syndrome. For example, Sekuro hosts CxO Tribe events, which bring together leaders in the community within a safe space, so like minded members can relax, and share concerns and experiences. It's a small step to making the industry a better and more collaborative space for everyone.

Interestingly, over a quarter (28%) of people said their mental health suffered due to remote working, ostensibly as a result of social disconnection from peers for long periods of time, or the blurring of work/home boundaries resulting in longer working hours.

What is keeping cyber security professionals up at night?

Q: What is your greatest worry at the moment?

Notably, for many cyber security professionals, experiencing a cyber attack isn't their biggest worry — it's unrealistic expectations from the board/ executive leadership that are keeping them up at night.



Note: 91 of the 101 participants answered this question

sekuro

Noel's Advice

"The survey results clearly show how important a cyber-aware board and leadership team can be in reducing stress amongst more junior team members. There's a real knack to communicating cyber security priorities in an 'upward' manner to executive leaders, but there's also a massive impetus for the leaders themselves to take genuine interest in and invest in company-wide cyber policies.

"Any of the major data breaches over the past few years, and their massive legal, financial, and reputational implications should be enough to give the cyber security team the gravity they deserve.

"Organisations are experiencing increasing demands from their customers for digital products and services, whilst also facing more sophisticated threats from cybercrime. This is a delicate balancing act that often leads to stretched technology teams or making do with under-trained members of existing teams.

"Outsourcing to trusted local partners can be a cost-effective and efficient way to bolster support for your overworked team."[5]

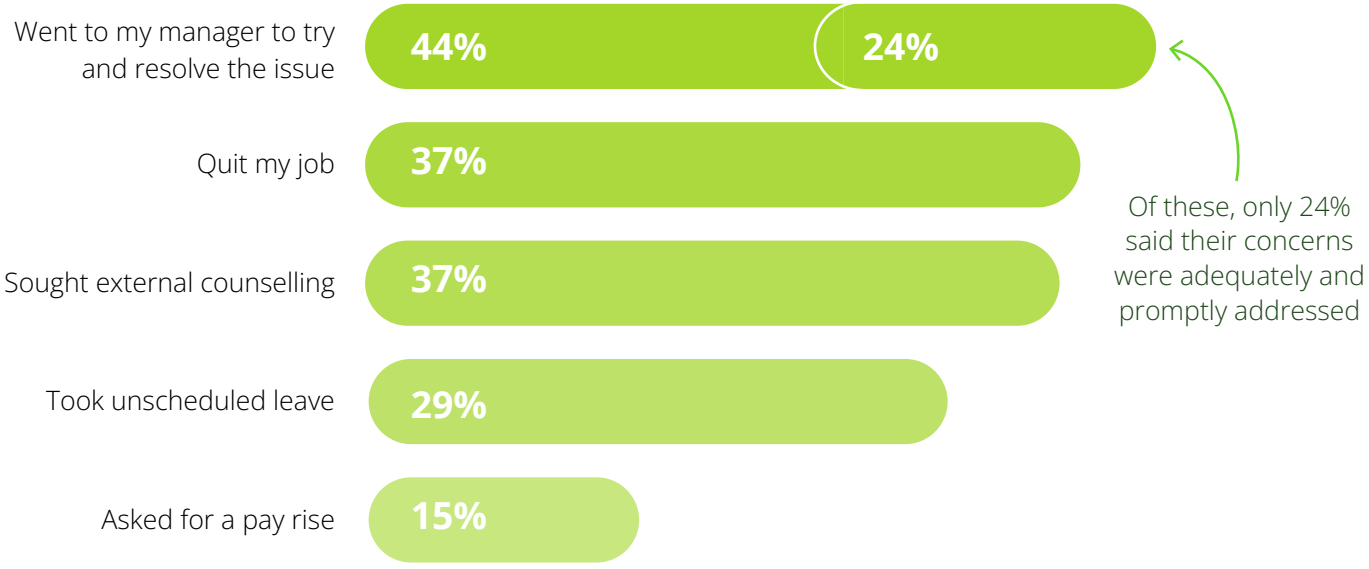
5. Sekuro's Team Augmentation Division and Virtual CISO offerings are designed to fill short to medium-term skills needs, alleviating pressure on internal teams.

Communicating concerns and accessing support

Workplaces must prioritise the mental wellbeing of their employees by offering streamlined and effective support services to everyone, from graduates to CEOs.

With talent retention set to be an ongoing issue, organisations should prioritise nurturing a positive and collaborative culture within the teams and perform regular check-ins both in person and through technology like pulse surveys. Additionally, always involve employees in meaningful and purposeful work, allowing them to value add and challenge themselves.

Q: If you have experienced mental health issues in the past two years, what actions did you take?



> "It's vitally important to seek support in difficult times. Whether this is a discussion with your colleagues, speaking to your manager or engaging with a mental health professional, the need to share and receive meaningful support is key to our ongoing wellbeing. Even if you're the type of person who is self-sufficient and doesn't experience workplace stress often, everyone needs, and benefits from, extra support from time to time. Prevention is always better than recovery. " says Amber Rules.

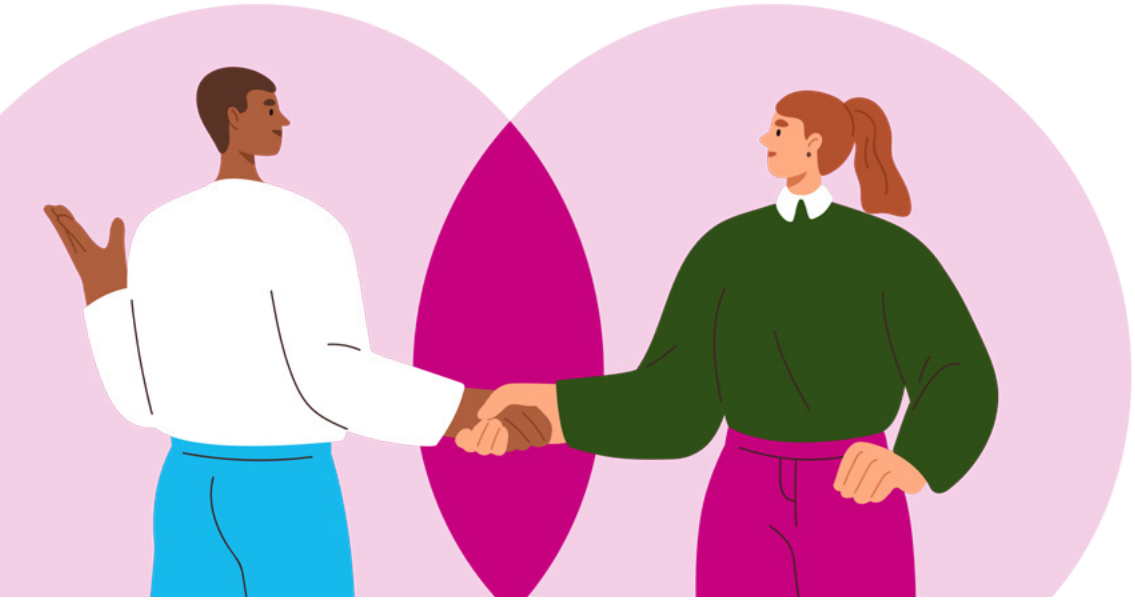
sekuro

The impact on the cyber security industry overall

Whilst it may seem like a small number, 9% of respondents said they quit their job and changed careers in response to mental health challenges. As of 2021,[6] there were 134,690 cyber security workers in Australia. If this trend is reflected industry-wide, that means over 12,000 cyber security professionals could have left the industry over the past two years.

The survey also demonstrated that simply handing employees more money would not solve their grievances. **Only one-fifth (22%) said a pay rise or promotion would help their mental health**, with many more citing the provision of more resources and tools or more frequent opportunities to provide feedback to management.

This demonstrates the need for greater mental health awareness in the industry, at both a leadership and staffing level, as well as enhanced skills development in the industry — as opposed to a tokenistic offering of higher pay.



6. (ISC)², 2021. *Cybersecurity Workforce Study*. [online] p.5. Available at: <https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx> [Accessed 29 September 2022].

Seeking future resolutions

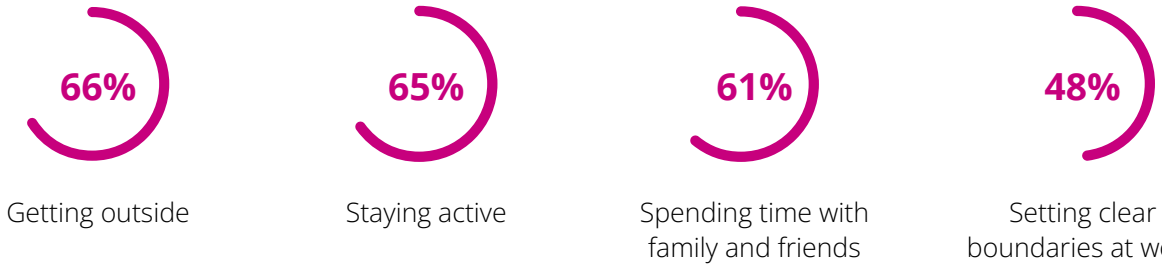
While it's clear respondents have some good tools to reduce poor mental health, there are other easy and practical ways a workplace can take an active involvement in improving the mental health of its employees. Encouraging group time away from screens to engage in mindfulness activities like meditation, breathwork, or light group exercise can be small gestures with big impacts.

With more than half of respondents not setting clear boundaries at work, it's time to integrate this mentality into daily life at your workplace. Setting boundaries personally, and encouraging employees and colleagues to do so too, is a fundamental way to protect yourself and work at a pace and in a style that best suits your preferences.

As more workplaces destigmatise having open conversations about mental health, the cyber security industry is well-placed to start a proactive journey to improving the mental wellbeing of its people. Leadership teams must recognise that good mental health can help individuals be better equipped to handle high-pressure situations, be more resilient, and more productive.

Q: If your employer could do one thing to improve mental health amongst its staff, what would it be?

Q: What helps you recover from/prevent mental health issues?



sekuro

Amber's Advice

"Building self-care into the culture of an organisation is essential for a mentally-well workforce. Providing opportunities for time away from screens and mindfulness activities is a great start, but organisations must also offer learning opportunities to their entire workforce that develop emotional intelligence and the capacity for clear and respectful communication, distress tolerance skills, and the ability to think critically about what is required to build an ongoing, robust culture of mental wellbeing.

"The concept of boundaries and boundary setting can be tricky. Many people may only have a vague understanding of what boundaries are, and perhaps have difficulty knowing how to set them in ways that respect both themselves and others. Organisations can support their employees' mental wellbeing by providing opportunities to discuss the concept of boundaries in the work context, and learn more about the specifics of boundaries. Employees will benefit from open, ongoing conversations and learning about boundaries alongside management.

"The good news is that proactive mental wellness support for staff promotes retention. If employers invest in helping staff build emotional intelligence and resilience, it's a win/win for staff and employers."

If you or someone you know is in crisis and needs help now, call triple zero (000). You can also call Lifeline on 13 11 14 — 24 hours a day, 7 days a week.

Sekuro is a cyber security and digital resiliency solutions provider that helps CIOs and CISOs take a strategic approach to cyber security risk mitigation and digital transformation. Operating at the intersection of the digital technologies and cyber security industries, Sekuro reduces cyber risk while new technologies are adopted — ultimately building business resiliency and enabling fearless innovation.

Our five practice areas (Governance, Risk and Compliance, Technology and Platforms, Offensive Security, Team Augmentation, and Managed Security Services) are full of the brightest minds in the industry. They work together to look beyond the threat landscape of today and into an opportunity landscape.

---

sekuro

L12, 234 George Street Sydney
2000 NSW, Australia
+61 1800 735 876 (1800 SEKURO)
info@sekuro.io
sekuro.io

For media queries, contact us at
media@sekuro.io