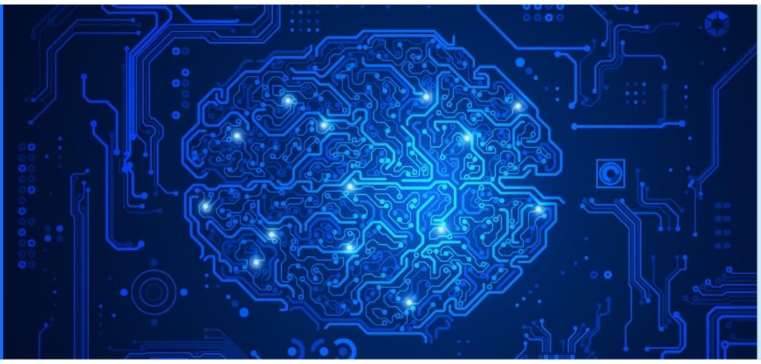
Cyber
Insights
Series



NSW
GOVERNMENT

Executive Summary – Cyber Insights Series

As an initiative of the Hon Victor Dominello MP, Minister for Customer Service and Digital Government, the Cyber Insights Series brought together cyber security experts from government, business and academia to develop solutions to some of the biggest issues facing the industry. Its key objectives were to enable closer collaboration across the public and private sectors, and to ensure NSW Government is across industry best practice.

Six sessions were held in the first Cyber Insights Series, co-hosted by Cyber Security NSW and a relevant industry partner. In 2023 we will host a second Cyber Insights Series. If you would like to submit topics or be involved in the 2023 series, please email info@cyber.nsw.gov.au.

Beyond Essential Eight

This session aimed to ensure that NSW Government is across industry best practice when it comes to cyber security frameworks. Co-hosted by CyberCX, the discussion provided a wealth of insights into how NSW can lead cyber security in Australia, beyond the Australian Cyber Security Centre's Essential Eight risk mitigation controls. Roundtable participants reiterated that while the Essential Eight is useful for benchmarking progress, it is not the "be all and end all" and there is no single approach to cyber security – each organisation has a unique risk profile that they must consider.

NSW Government is looking into risk mitigation strategies beyond the Essential Eight, such as an innovation hub and policies for high-risk vendors.

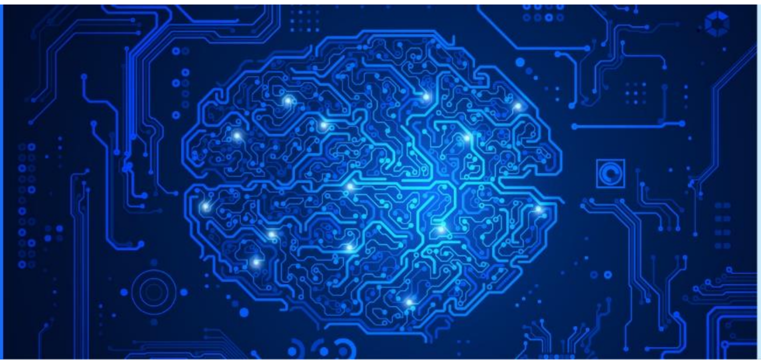
Reporting Metrics & Evidence of Impact

Co-hosted with CISO Lens, this session sought to explore how other organisations are measuring and reporting on cyber security metrics, and how this data is assisting cyber security uplift, in line with organisational objectives. Participants noted there is an art and science to cyber security reporting. It's more than just collating data – security teams need to translate meaning for leadership teams.

In 2022 Cyber Security NSW established the Cyber Insights & Performance team, which will use reporting metrics to identify whole-of-government risk and work closely with NSW Government entities to assess and mitigate their specific risks.

Vulnerability Disclosure

To leverage their expertise in this area, Cyber Security NSW brought on Bugcrowd, an Australian bug bounty and vulnerability disclosure company, to co-host this session. The central objective of this roundtable was to inform NSW Government's first vulnerability disclosure policy, which is currently being developed by Cyber Security NSW.



The roundtable identified the need for legislation to be amended, to ensure that those participating in good faith reporting within the guidelines of vulnerability disclosure policies are not liable to be prosecuted by legislation. Following the session, some of the academic and industry attendees drafted a paper on a ‘cyber socket’ that would allow organisations to create vulnerability disclosure programs that are aligned to the legislation.

Critical Infrastructure

Led by Deloitte, this session explored how NSW Government can complement the Commonwealth’s Security of Critical Infrastructure Act to improve cyber security protections for NSW’s critical infrastructure. A prominent theme over the course of the discussions was that cyber security risk is a whole-of-organisational risk. It therefore needs to be integrated into business continuity and led from the top-down, with leadership teams taking ownership and responsibility.

To foster this cyber safe culture in NSW Government’s leadership teams, Cyber Security NSW has developed cyber security awareness training e-modules tailored for executives, which are available across NSW Government.

Women in Cyber

For this session, Cyber Security NSW heard from women leading the cyber security industry to those who are just starting out in the field, about how NSW Government can more effectively attract, train and retain female cyber security specialists.

A number of women said that shifting the perception of cyber security – through greater representation (especially at the leadership level), flexible work practices and mentorship programs – would help encourage more women to join the industry. To support their great work in fostering a connected community of female professionals, NSW Government has become a gold sponsor of the Australian Women in Security Network, who co-hosted this session.

To upskill NSW Government’s existing female cyber security workforce, Cyber Security NSW is sponsoring 11 women working across a range of clusters to undertake a cyber security course up to the value of $15,000.

Protecting Mental Health

At this session, we heard from around 60 cyber security leaders about how their teams are coping, which confirmed what we already knew – the industry is feeling overwhelmed and burnt out. NSW Government has sponsored the session’s co-host, Cybermindz.org – a not-for-profit that specialises in building mental resiliency in the cyber security industry. In 2023 Cyber Security NSW will trial Cybermindz.org’s eight-week program to build mental resiliency. The branch is developing further support structures and investigating options that could be rolled out across NSW Government.