Impact Case Study

The Australian Cyber Security Skills & Jobs NSW Study

Introduction and background

In early 2020, the Australian Information Security Association (AISA) partnered with NSW Treasury to undertake a research project that would identify potential cyber security skills gaps and look at the impact of COVID-19 on the local cyber security industry.

The project was led by AISA and the research aspects of the project were a collaboration between Professor Matthew Warren, the director of the RMIT University Centre for Cyber Security Research and Innovation (CCSRI) and Damien Manuel, Chairman of AISA and Director of Deakin University's Centre for Cyber Research & Innovation (CSRI).

When the coronavirus pandemic broke out in early 2020, physical health wasn't the only area of public wellbeing at stake. Lockdowns to prevent the spread of Covid-19 were accompanied by a rapid escalation of remote working and schooling.

This sudden and large-scale shift online meant that individuals, businesses, organisations and schools had to respond swiftly – without additional resources and within existing budgets – to attempt to ensure that their cyber security was robust and effective.

In response to this need, AISA and the NSW Treasury commenced the Australian Cyber Security Skills & Jobs NSW Study to identify potential cyber security gaps and examine the impact that the pandemic was having on the local cyber security industry.

The research

A first part of the study was to understand the impact of the pandemic by interviewing key stakeholders, and so define the research parameters.

Once interviews were completed and the issues identified, AISA surveyed its 6,500+ individual and corporate members to learn how Covid-19 had affected their work – including working hours, skill shortages, work flexibility, workforce diversity, and whether remote working was effective.

Interviews and surveys of CISO, CSO, CIO and business executives and recruiters were conducted across the following sectors:

- Aerospace
- Banking and Finance
- Critical Infrastructure (power, energy, water and other utilities)
- TAFE / Tertiary
- Government agencies (State / Federal)
- Manufacturing
- Not-For-Profit
- Retail
- Telecommunications
- Managed Service Providers (MSPs) Cyber security vendors.

Details of positions requiring information security skills advertised in Australia on Seek.com between January and June 2020 were also collated.

Funding support and institutional support

The project was funded by the NSW Treasury. AISA also interviewed the main stakeholders to establish how to approach the project.

What's next...

RMIT UNIVERSITY

Project outcomes

The final report – The Australian Cyber Security Skills & Jobs NSW Study – report can be downloaded at: https://www.business.nsw.gov.au/__data/assets/pdf_file/0007/385549/ATTACHMENT-C-AISA_NSW-Report_2020_Final-5.pdf

AISA's member survey found that in NSW:

- 96.5 per cent of NSW cyber security staff to work from home (WFH)
- 3.5 per cent of staff stated that they were employed in roles that did not allow a WFH model.

Of those who were employed pre-COVID-19:

- 70.4 per cent had experienced no change in their working status amid closures and physical distancing measures
- 7.8 per cent either were laid off, quit their job or had their employment contract terminated.

Other findings included:

- 96.5% were working from home
- 34.4% were working longer hours post-COVID-19
- 12.6% had their income negatively impacted post-COVID-19
- 70% of cyber security professionals have an industry accreditation
- 52.6% believe gender diversity in the sector has improved
- 13.9% of workplaces actively integrate autism / neurodiversity

From an executive perspective, 80% of executives believed their organisations are under-resourced. The main constraints to hiring sufficient staff were identified as:

1. Budgetary constraints (81.3%)
2. Headcount freeze (62.5%)
3. Unable to meet demand due to the continual increase in the threat landscape, (31.3%)
4. The inability to find the right talent in the market (25%).

Overview of the impact

In the final report, AISA noted:

"With crisis comes opportunity and, since social distancing measures were put into place, organisations and small business have been forced to become more agile, innovative and quick in decision-making and execution. The local security industry — as summarised in this report — will face new challenges in a post-COVID economy, but it is also an opportunity to educate, innovate and promote awareness."

Speaking of the study's impact, Stuart Ayres, the NSW Minister for Jobs, Investment, Tourism and Western Sydney, said:

"The Australian Cyber Security Skills & Jobs NSW Study commissioned by the NSW Government, brought important insights to light. Those insights have informed the NSW Government's Cyber Security Strategy. Importantly, the strategies for addressing job and skills gaps may benefit from greater diversity in the workforce."

The 2021 NSW Cyber Strategy outlines key strategic cyber security objectives, guiding principles and high-focus areas for the NSW Government to apply to future work programs.

See the 2021 NSW Cyber Strategy (with $240m funding over 3 years) at: https://www.digital.nsw.gov.au/transformation/cyber-security/cyber-security-strategy

Next steps

After the success of the NSW study, the Victorian government has approached RMIT to undertake a similar study as part of its Victorian Higher Education State Investment Fund (VHESIF) Digital CBD project.

What's next...