AISA

THE AUSTRALIAN CYBER SECURITY SKILLS & JOBS **NSW STUDY**

SEPTEMBER 2020

www.aisa.org.au

CONTENTS

FIGURES

AISA

The Hon. Stuart Ayres, MP
Minister for Jobs, Investment, Tourism and Western Sydney

MINISTERIAL FOREWORD

NSW strives to enhance the cyber security sector by strengthening skills and growing the industry talent pool.

The rapid progress of technology continues to drive digital connectivity, and in recent times COVID-19 has driven a sharp increase in remote online activities. This environment has catalysed the creation of inlets for cyber threats penetration, and cybercrime is increasingly a significant risk to business.

At the forefront of digital technology and innovation is our people. The ability for NSW to build the skills of the future to support a strong cyber security sector is paramount to increasing international competitiveness.

I thank the Australian Information Security Association for its comprehensive research and analysis to provide a clear picture of cyber security skills in NSW during a time in which mounting pressure of health and cyber threats has caused economic uncertainty.

The study's finding has brought some important insights to light that will inform the NSW Government's current industry development work for the sector. Of importance will be taking steps to address the job and skills gap, with potential for the latter to benefit from greater neuro and gender diversity.

I am delighted that the report has also confirmed the viability for cyber security professionals to work from home which has the potential to expand the footprint of cyber jobs, and in doing so transforming the NSW regional economy.

I welcome the findings of this report which will provide valuable input to the development of the forthcoming 2020 NSW Cyber Security Strategy.

The Hon. Stuart Ayres, MP
Minister for Jobs, Investment, Tourism and Western Sydney

AISA

FOREWORD FROM AISA

> ***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.***

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.

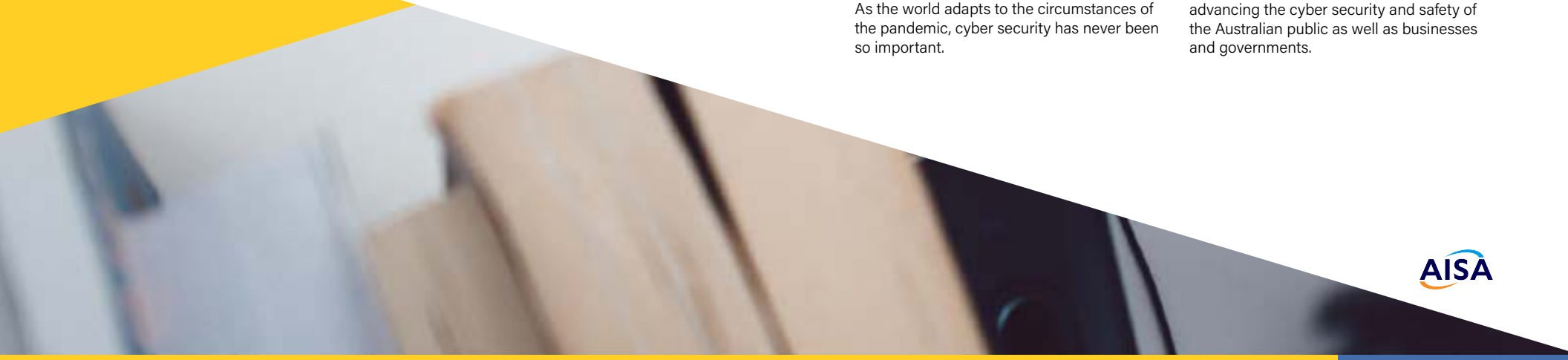
When faced with the rapidly changing and escalating public health emergency of COVID-19, cyber security professionals answered their call to service and stood front and centre to support and protect their organisations as this crisis unfolded.

Organisations and staff have worked tirelessly to move to remote working and schooling. Many organisations have spent additional resources (without receiving additional budgets) to protect their systems. As the world adapts to the circumstances of the pandemic, cyber security has never been so important.

AISA is proud to bring to you the Cyber Security Skills & Jobs NSW Study 2020. We trust it provides you with an understanding of the current state of the NSW sector — advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia.

About the Australian Information Security Association (AISA)

The Australian Information Security Association (AISA) is the peak body for information and cyber security professionals. AISA champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments.



EXECUTIVE SUMMARY

AISA's survey of members found that in NSW, of those who were employed before COVID-19, 70.4 per cent had experienced no change in their working status amid COVID-19 closures and physical distancing measures, while 7.8 per cent either were laid off, quit their job or had their employment contract terminated.

AISA also found that 34.4 per cent of NSW respondents had experienced longer working hours post COVID-19, while 11.8 per cent had experienced a reduction in their working load. Overall, 77.1 per cent of cyber security professionals surveyed were somewhat satisfied to very satisfied with their job.

Only 2 per cent believed they had too many cyber security staff while 28.9 per cent believed they had the right staffing levels.

When members in executive roles were surveyed on the impact of COVID-19, 80 per cent in NSW reported their organisations were under-resourced, including 15 per cent who stated they were very under-resourced.

On neurodiversity, 13.9 per cent of NSW respondents reported workplaces that actively integrated individuals with autism/ neurodiversity. Gender diversity in the workplace relating to cyber security was reported by 52.6 percent in NSW to have either significantly increased or improved.

Regarding job advertisements, there were 484 cyber security positions posted online via Seek.com.au in May and 508 in June 2020, Australia-wide. New South Wales accounted for 142 of those in May and 189 in June, indicating a steady increase.

13.9%
of workplaces actively integrate autism / neurodiversity

80%
of executives believe their organisations are under resourced

12.6%
had their income negatively impacted post COVID-19

34.4%
are working longer hours post COVID-19

7.8%
of cyber security professionals have lost jobs since COVID-19

70%
of cyber security professionals have an industry accreditation

52.6%
believe gender diversity in the sector has improved

96.5%
are working from home

CYBER SECURITY PROFESSIONALS: A PERSPECTIVE

Prior to the impacts of COVID-19, 87 per cent of NSW cyber security respondents were employed full-time, while only 6.1 per cent were part-time or casually employed in cyber security. Approximately 2.6 per cent were unemployed.

The COVID-19 Impact To Jobs

Post COVID-19, of those employed, 70.4 per cent have seen no change in their working status, while 7.8 per cent either were laid off, quit their job or had their employment contract terminated. As revealed in the survey data, 12.6 per cent of respondents in NSW experienced negative consequences due to COVID-19 either through reduced paid hours, reduction in salary or moving from full-time to part-time. On the positive side, 2.2 per cent of professionals have experienced a salary increase overall, while an additional 2.6 per cent had increased their paid work. Interestingly, during a period of workforce pressures, only 3 per cent of respondents in NSW have changed their job which is very similar to the national numbers across all states. Of those surveyed, ACT stood out as having more of the workforce changing jobs post COVID-19 at 10.5 per cent, while Victoria was more stable at 1 per cent.

Looking at the working week for cyber security professionals who are employed in NSW post COVID-19, 34.4 per cent have experienced longer working hours while only 11.8 per cent have experienced a reduction in their working load. The frequency of additional hours varies greatly from a few extra hours a day to extremes of 40 per cent increase in the total number of hours worked in a given week. Regardless of the additional hours worked in a given week, 77.1 per cent of cyber security professionals are somewhat satisfied to very satisfied with their job.

There appears to be ample capacity for new entrants into the cyber security workforce in Sydney, assuming businesses are not holding back hiring to manage finances. The study found that 60.7 per cent of professionals in NSW believe they have some type of shortfall in the number of staff working in cyber security within their organisation. Only 2 per cent believe they have too many cyber security staff while only 28.9 per cent believe they have the right numbers of staff to adequately protect their organisation. The remainder (8.5 per cent) are undecided or preferred not to comment.

While the cyber security sector is not immune to the negative impacts of COVID-19, the sector's resilience and robustness due to a combination of factors has resulted in minimal job losses compared to the rest of the economy.

The key factors are:

- **Continued skill shortages,**
- **Flexibility with working location, and**
- **Increasing external hostile threats to both businesses and government**

Working Status Prior to the Impact of COVID-19

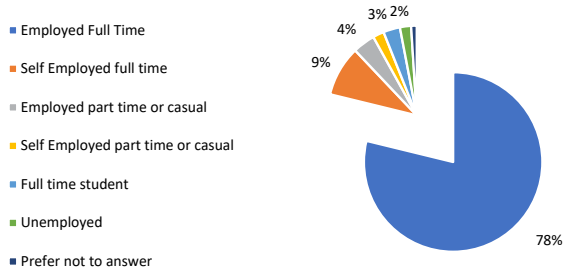


Figure 1 | Working status prior to the impact of COVID - 19

Working Status Post COVID-19

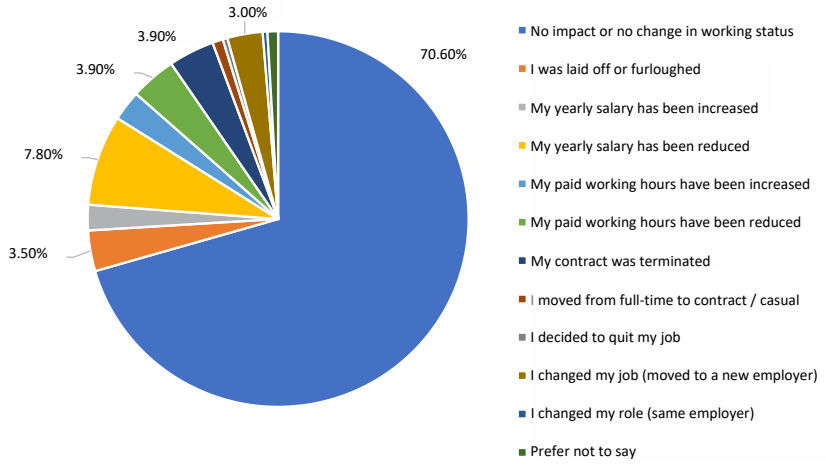


Figure 2 | Working status post COVID - 19 Impact

Can Cyber Professionals Work Remotely?

The COVID-19 pandemic forced 96.5 per cent of NSW cyber security staff to work from home (WFH) while 3.5 per cent of staff stated that they were employed in roles that did not allow a WFH model. Of those who could WFH, 7.3 per cent stated they would like to continue to work from home all the time post-pandemic, 51.3 per cent preferred to work from home most of the time and 38.8 per cent responded they would like to work from home sometimes. Only 2.6 per cent of NSW cyber security staff indicated they prefer to not work from home at all. The 58.6 per cent of respondents who would work from home all the time to most of the time, represents significant job opportunities for remote and regional NSW with stable power and access to high speed broadband Internet (e.g. NBN Home Standard or higher).

Does remote working actually work?
Working from home, however, does have some drawbacks for the workplace, resulting in increased tensions, miscommunications and escalation of items which would have otherwise been resolved quite easily face to face. The drawback of working from home has led to 21.1 per cent of NSW respondents experiencing a degradation in workplace communication with co-workers.

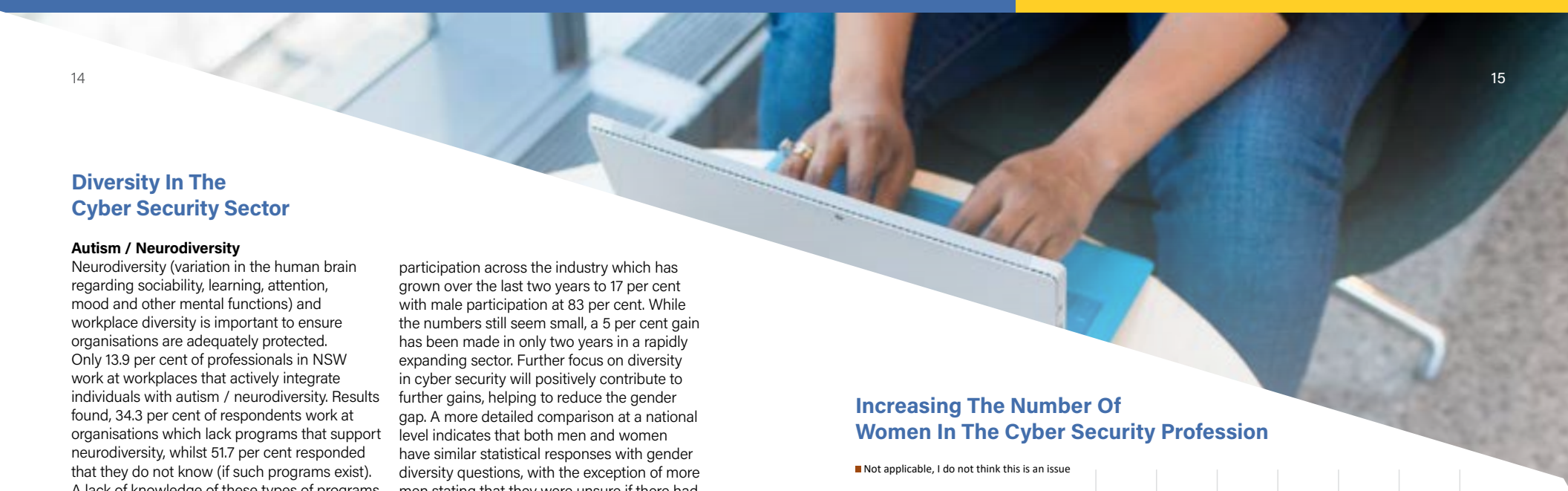
In contrast to this, 27.3 per cent have experienced a positive impact which has improved co-working communications. This is most likely due to people communicating in more personal settings (e.g. viewing the background of people's homes) which has enabled additional conversation points and a different perspective on the individual as people tend to have items on display which define them (e.g. family photos, books, awards, art, etc..).

Results also found that 47.9 per cent of the NSW cyber professionals reported no negative or positive change in communications with co-workers, (net neutral).

It should be noted that the data was collected once schools had reopened and there is anecdotal evidence from conversations with various cyber professionals that prior to schools reopening, parents (single or family) with children in primary school, struggled to balance child home education (e.g. reading, writing and keeping the children constructively occupied) with work life adding stress and tension. In the analysis, 3.6 per cent of cyber professionals did not want to comment or felt unsure if there was a positive or negative change.

The 3.5% of cyber professionals who have not worked from home throughout COVID-19 are in roles that prohibit them from doing so.

AISA



Diversity In The Cyber Security Sector

Autism / Neurodiversity
Neurodiversity (variation in the human brain regarding sociability, learning, attention, mood and other mental functions) and workplace diversity is important to ensure organisations are adequately protected. Only 13.9 per cent of professionals in NSW work at workplaces that actively integrate individuals with autism / neurodiversity. Results found, 34.3 per cent of respondents work at organisations which lack programs that support neurodiversity, whilst 51.7 per cent responded that they do not know (if such programs exist). A lack of knowledge of these types of programs demonstrates more needs to be done to broaden the conversation in the sector to drive positive change and benefits. Victoria has more employees at organisations with neurodiversity programs (24.6 per cent) compared to NSW (13.9 per cent) and the national average is 18.3 per cent.

Gender Diversity
Gender diversity in the workplace relating to cyber security indicated that 52.6 per cent of respondents consider that diversity has improved or increased. Only 26.1 per cent believe it has stayed the same, with only 1.7 per cent believing diversity to have slightly decreased. A further 19.1 per cent were unsure if there had been an improvement or deterioration of the number of women participating in the sector.

An analysis of the sector by AISA two years ago showed that approximately 12 per cent of the sector are women. The current Jobs and Skills analysis undertaken by AISA in NSW had a response rate of 18.3 per cent women, 79.1 per cent men, 0.4 per cent who preferred to self-describe and 2.2 per cent who preferred not to specify a gender. The national response rate by gender was 16.1 per cent women, 80.8 men, 0.3 per cent prefer to self-describe and 2.8 per cent prefer not to disclose. Based on the response rates, it appears female participation in the sector has improved slightly. This can be confirmed by the increase in female participation across the industry which has grown over the last two years to 17 per cent with male participation at 83 per cent. While the numbers still seem small, a 5 per cent gain has been made in only two years in a rapidly expanding sector. Further focus on diversity in cyber security will positively contribute to further gains, helping to reduce the gender gap. A more detailed comparison at a national level indicates that both men and women have similar statistical responses with gender diversity questions, with the exception of more men stating that they were unsure if there had been an improvement or decline (21.3 per cent men vs 14.9 per cent women).

Is a professional qualification required in order to be employed?
When examining the number of cyber security professionals with global industry relevant cyber security accreditations / certifications that were either vendor agnostic or vendor based, 74.4 per cent of participants reported they hold valid accreditations/ certifications whilst 25.6 per cent do not. Nationally, 70 per cent held valid accreditations/ certifications while 30 per cent did not (almost 1 in 3).

A majority of cyber security professionals (52.51 per cent) in NSW believe the industry should be regulated and accredited by an independent organisation, ensuring a base level of qualification and standard in the industry (as with Engineers Australia, the Australian Medical Association and the Law Society of NSW). Across the country, the majority of cyber security professionals (55.2 per cent) share this view. It should be noted that the position of regulating cyber security professionals has decreased from a high of 68.6 per cent support in the industry prior to COVID-19. Slightly less than half (47.4 per cent) of cyber security professionals in NSW either object or don't know if the industry should be regulated. Prior to COVID-19, 31.4 per cent of professionals across the country objected to the introduction of regulation of professionals in the sector.

Increasing The Number Of Women In The Cyber Security Profession

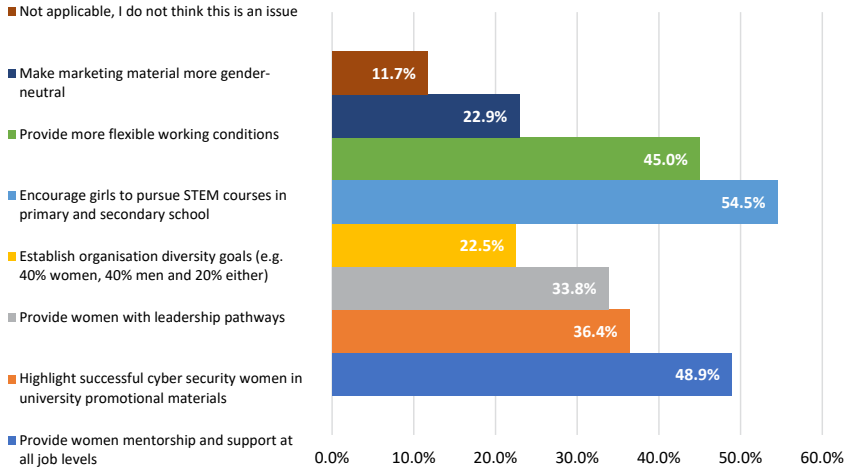


Figure 3 | Increasing the number of women in the cyber security profession

When are cyber security certifications the most helpful?
Cyber security certifications / accreditations are most useful to NSW cyber professionals when they are looking for an advancement opportunity outside of their current organisation (33.9 per cent). New starters to the industry find certifications / accreditations useful at the beginning of their cyber security career (21.1 per cent) with a smaller group (13.2 per cent) finding them useful before getting their first job in the sector. It is interesting to note that only 14.5 per cent of NSW cyber professions find industry certifications / accreditations important when looking for an advancement opportunity within their existing organisation. In NSW, 17.2 per cent of cyber security professionals don't see certifications as useful (i.e. just a hurdle in the employment process) or are unsure how helpful they have been in their career development. This may be due to the very large number of both vendor and vendor agnostic industry certifications / accreditations that already exist across the sector that are of varying quality and content.

Building Skills For The Future

Investment in cyber security training and education is expected to increase over the next 12 months. Almost 60 per cent of respondents are optimistic of such an increase with only 9 per cent expecting a decline. The remainder of those surveyed were uncertain whether the level of investment for training and education of staff would change.

This optimistic outlook indicates a shift to reinforce skills during a time of uncertainty in the market. This optimism however, is offset by the 38.7 per cent of NSW cyber professionals concerned that security spending for personnel (hiring) will be negatively impacted this year because of lost revenue suffered by organisations due to the COVID-19 situation. It is anticipated this impact will become more visible in the market over the next 4 to 6 months (beyond September), when the Federal Government's JobKeeper scheme is adjusted. Despite the challenges of COVID-19, 38.2 per cent of NSW cyber security professions are optimistic about the current market conditions.

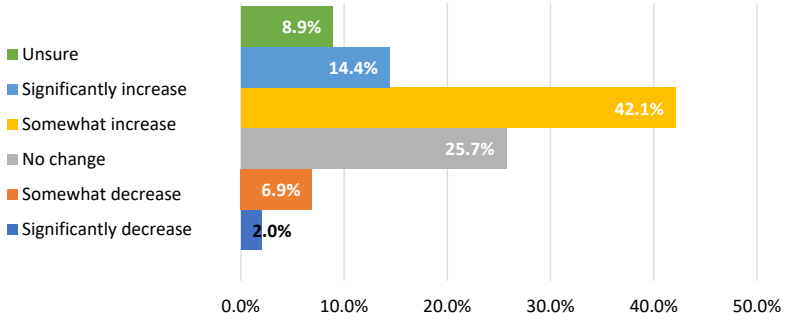


Figure 4 | Investment changes in cyber security training and education within the next 12 months

Investment Changes In Cyber Security Training And Education Within The Next 12 Months

Cyber security professionals in NSW want to further develop or improve a range of skills over the next two years to advance their career. The top three areas of focus for existing cyber security professionals are:

- Management and leadership skills;
- Technical hands on skills, and;
- Developing a broader knowledge base.

A very small number of respondents are considering marketing skills to assist with outreach communication.

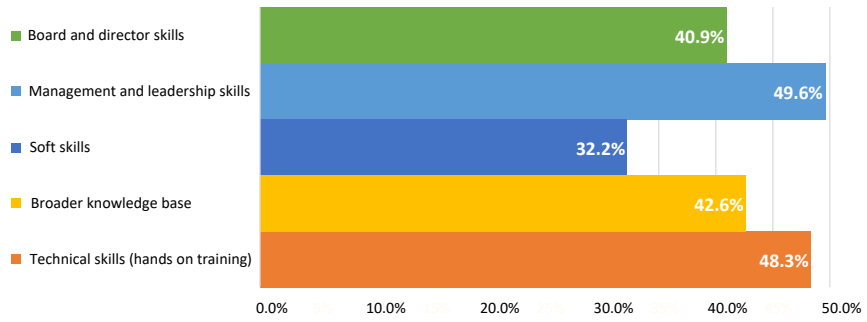


Figure 5 | Areas of focus for existing cyber security professionals

CYBER SECURITY EXECUTIVES: A PERSPECTIVE

What is holding back jobs growth post COVID-19?
The top four main constraints preventing organisations from hiring staff have been budgetary constraints (81.3 per cent), headcount freeze (62.5 per cent), the continual increase in the threat landscape, hence unable to meet the demand (31.3 per cent) and the inability to find the right talent in the market (25 per cent). Other minor constraints which are not considered limiting factors, like those mentioned above, include rapid organisational growth through mergers and acquisitions (M&A – 12.5 per cent) or the redeployment of staff to other essential business activity as a result of COVID-19 (6.3 per cent).

Does the sector have enough skilled resources post COVID-19?
Prior to the impacts of COVID-19, executives responsible for cyber security within their own commercial organisations mainly reported their teams were under resourced and consequently unable to deal adequately with cyber threats. Only 20 per cent felt they were adequately resourced with enough cyber security staff to deal with the day to day challenges. Of the 80 per cent who indicated they were under resourced, 15 per cent stated they were very under resourced.

However, the impact of COVID-19 has not changed or increased the pressure on resourcing to the degree that was expected. This resulted in 80 per cent of organisations indicating that they are still not adequately resourced. However, digging deeper into the results through discussions, organisations which were already under resourced have continued to be under resourced. Reductions of staff numbers in cyber security have been through the loss of vacant positions and in some instances redundancies through organisational restructures to minimise business expenses, even in organisations which were very under resourced already.

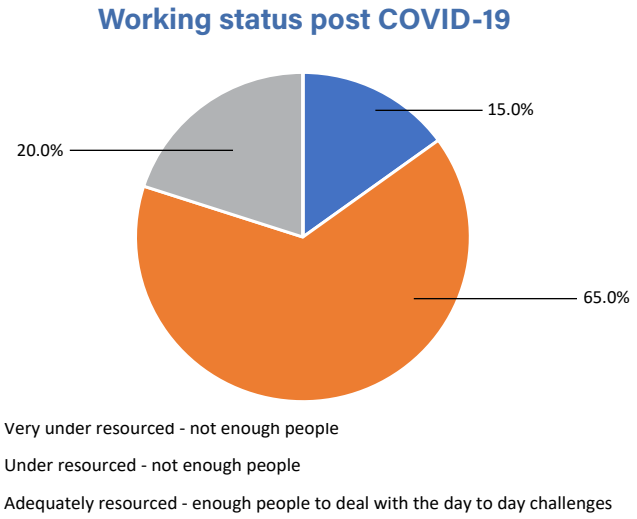


Figure 6 | Resources protecting organisations

Key Cyber Workforce Constraints
Some executives (12.5 per cent) felt they were unable to obtain the level of resources required to protect the organisation as upper management were not focused enough on cyber security risks and threats to the organisation. In some cases, organisations are looking for cost reductions across the business, regardless of business function. The types of cyber security jobs that have remained vacant or been lost include; analysts, cloud architects, junior positions (including graduates), cyber education and awareness advocates, data security analysts and security architects.

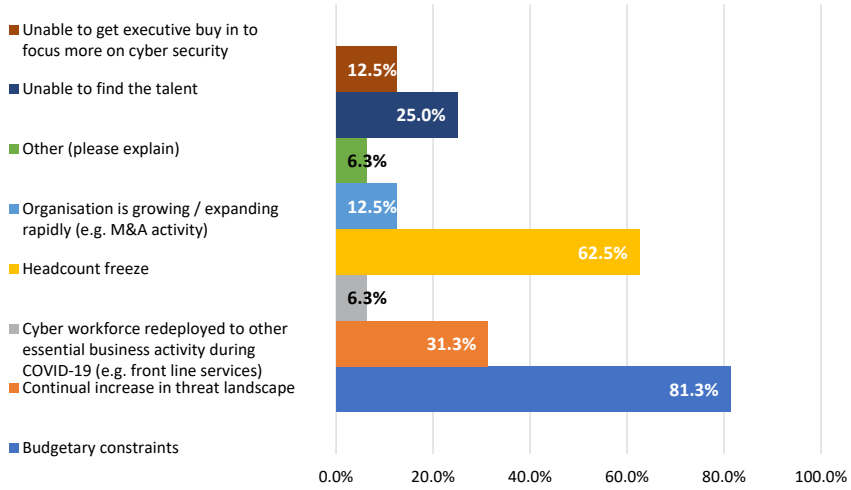


Figure 7 | Key cyber workforce constraints

CYBER SECURITY EXECUTIVES: A PERSPECTIVE (CONTINUED)

COVID-19 has also had a negative resourcing impact on 15 per cent of organisations who have actively reduced the size of their security teams. While any job losses are negative, the remaining 85 per cent of business have not needed to reduce their cyber security workforce. While 60 per cent of organisations have not changed their operational security budget, 20 per cent have had a reduction in their budget which will impact their ability to hire or purchase new systems / technology. The results also showed that 15 per cent of business felt it was too early to determine if there was a negative impact on their cyber security budget. For those who did report a negative impact on their budget, 75 per cent stated the budget impact was between 10-19 per cent (reduction), whilst a smaller portion of respondents (25 per cent) reported a budget impact which was up to 29 per cent.

Where is the skill gap for businesses?

Considering the existing cyber workforce capability within organisations, 50 per cent of executives felt the depth and breadth of skills within their existing teams is inadequate to protect their organisation. The majority of those executives felt they needed staff with more skills in "monitoring and incident management" (80 per cent) and "technical assurance" (60 per cent). A smaller number felt they needed more staff with architecture skills. Based on further analysis, it appears organisations have enough people with skills in compliance.

When asked which skills are difficult to attract and retain, executives responded that the most difficult to attract were "monitoring and incident management" and "architecture", with "monitoring and incident management" also the most difficult to retain. One of the main factors why businesses find it difficult to attract and retain staff is the level of pay expected in the sector, with a number of organisation unable to compete with the pay being offered at much larger organisations (e.g. financial services). Other key factors in relation to retaining staff is the challenge of burnout in a high pressure, high demanding role.

Executives responded that some roles are not promoted enough on the supply side, meaning a number of students simply don't gravitate or build skills for those desired roles. In other cases, the high demand for some areas seem to be related to the personality of people being more highly desirable. For example, people who are personable, good communicators and have a strong work ethic. While there may be plenty of people on the market in a particular field, finding individuals with the aforementioned soft skills is difficult (e.g. SecOps).

A key area for improvement within the business community is the establishment of graduate or internship programs to seek and assess new talent. This has several key benefits for businesses:

- Provides employers with a "try before you buy" model to test talent over a 3+ month period, particularly during an internship involving students in their final year of study. Typically, 67 per cent of students who undertake an internship will be hired by the host organisation.
- Acquiring talent from the tertiary sector acts as a handbrake on wage growth, making it more affordable for more organisations to hire the skills they require. It should however be noted that businesses will need to provide newly employed graduates with incentives (e.g. work life balance, extra-curricular training, a defined career progression path etc.) to retain them as they may become targets for poaching by other organisations.
- Dealing with tertiary sector and TAFE NSW, businesses save on recruitment fees. This saving would enable businesses to structure the cost saving as a bonus or incentive plan to retain the newly employed talent.
- Directly working with the tertiary sector or TAFE NSW enables businesses to influence course outcomes and teaching material, improving outcomes for both students and business by reducing the ramp time required to adjust to a business environment.

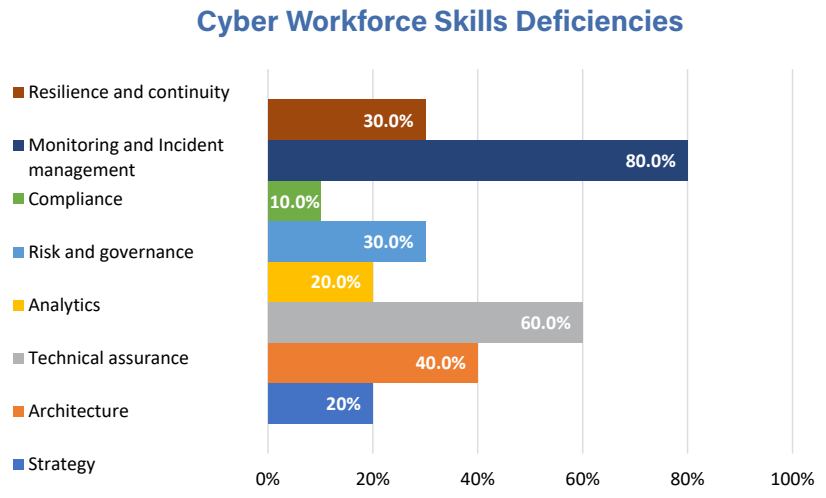


Figure 8 | Cyber workforce skills deficiencies

In cyber security, diversity of thinking, or neurodiversity, has provided a number of larger organisations with major benefits, particularly in regards to problem solving, identification of threats or hunting adversaries within networks and applications. The study indicated that only 20 per cent of businesses actually have a neurodiversity program while 60 per cent do not have a defined program and 20 per cent were unsure if a program existed within their organisation.

There is increasing evidence that the coronavirus pandemic has permanently changed the way organisations function and deliver their services. A majority (80 per cent) have moved to remote working for all employees, or a work from home (WFH) model and some (20 per cent) have only been able to enable some of their employees to work from home. In technology-driven sectors or where services can be offered remotely, businesses have naturally moved to the WFH model. Organisations which still need to provide human front line services (e.g. retail, banking etc..) have adopted a hybrid model. Staff who don't need to deal physically directly with customers tend to work from home (e.g. project staff, IT services, cyber, education etc) and staff who do deal directly with customers, but can transition to video conferencing have opted to do so. Only a small portion of front-line staff have had to continue to work physically in the workplace rather than transitioning to WFH.

The survey showed that 5 per cent of organisations will continue to allow employees to continue to work from home all the time; 35 per cent of organisations will allow staff to work from home most of the time and a majority of respondents (50 per cent) will still have an office presence requiring staff to work from the office, but have some flexibility to WFH, once the pandemic has passed. The survey also showed that only 5 per cent of respondents will require staff to work in an office location 100 per cent of the time. It should be noted that 5 per cent of respondents were unable to make a decision on the working conditions at this time.

The analysis also investigated the average size of security teams. While banking and finance sectors have teams of between 300 to 600 staff dedicated to cyber security a majority of organisations (40 per cent) typically have cyber security teams with between 5-14 dedicated cyber security staff. A further 20 per cent of respondents have larger teams in the order of up to 29 staff. There was no correlation between organisation size (e.g. number or full-time employees) and the number of cyber security staff employed. There was a correlation based on industry sector, highlighting that some sectors are more focused or negatively impacted by cyber breaches.

CYBER SECURITY EXECUTIVES: A MANAGED SERVICE PROVIDER (MSP) AND CYBER SECURITY VENDOR PERSPECTIVE

Cognisant that there are different segments of the cyber security industry, AISA also assessed Managed Service Providers (MSP), Integrators and Cyber Security Vendors, referred to as Service Providers, to better understand how they fared compared to the rest of the business community in Australia. This was important as some providers of services are Australian based entities with headquarters in Australia, while others are international based organisations with sales, support, engineering and consulting teams based in Australia. Prior to COVID-19, 62.5 per cent of Service Providers felt they were adequately resourced to service the needs of Australian customers. Only 25 per cent felt they were under-resourced in some areas (e.g. internal cyber staff, support staff and customer facing staff such as sales) while 12.5 per cent elected not to disclose.

What has been the impact of COVID-19 to MSP and cyber security providers?

Following the COVID-19 pandemic the situation has changed with only 12.5 per cent stating they were under-resourced, 75 per cent adequately resourced with enough people to deal with the day to day challenges with 12.5 per cent indicating they were now over resourced, mainly due to market conditions relating to COVID-19 (e.g. budgetary constraints and customers less focused on cyber security). If there were no business constraints, Service Providers would want to hire people with consultancy, analytics and engineering skills to better serve the market and their customer base. Unfortunately, one in four Service Providers have had to reduce the number of staff due to COVID-19, indicating a contraction in this segment of the industry. Service Providers and MSPs only reduce staff numbers when they are unable to meet expected sales targets. This indicates their sales targets under COVID-19 conditions are unobtainable (e.g. less spending by customers), or they function in a market segment which isn't positively impacted by COVID-19 (e.g. positively impacted segments include cloud-based services, business optimisation services, services to facilitate conferencing and WFH).

A majority of Service Providers felt their workforce contained the right depth and breadth of skills (62.5 per cent). Only 37.5 per cent of Service providers felt they had teams without the right mix of skills. This is considerably lower than commercial organisations who were evenly split (50 per cent) about their existing workforce capabilities.

Where is the skill gap for MSPs and cyber security vendors?
Service providers felt their teams were mainly deficient in four core areas: Strategy, Risk & Governance, Compliance, and Consultancy. Comparing this with businesses, they had three key areas of deficiency, which were (in order): Monitoring & Incident management, Technical assurance, and Architecture.

In terms of attracting and retaining staff, Service Providers found it most difficult to attract and retain people with skills in: Strategy, Risk & Governance, Compliance and Consultancy. Some providers commented, skills overseas in these areas were of a higher calibre due in part to the larger market with greater opportunities for varied experiences to be gained. Only one in four Service Providers reported they have a cyber security graduate / internship program to draw upon as a source of talent. For organisations that did, they indicated that they would only employ one to two graduates a year. In regards to neurodiversity programs, only 12.5 per cent of organisations have a program to integrate autistic or neurodiverse individuals into the workforce, with the remainder stating they didn't have a program and a quarter stating they were unaware of a program in their workplace.

12%
Are under resourced post COVID-19

75%
Are adequately resourced post COVID-19

12%
Are over resourced post COVID-19

25%
Staff reduction post COVID-19

Is WFH viable for MSPs and service providers?
All Service Providers interviewed have moved to the WFH model with 75 per cent moving all staff to WFH. When a solution has been found to eliminate the need to WFH and social distance, 12.5 per cent of providers will continue to have staff working from home most of the time with the majority providing their staff with the flexibility to WFH sometimes.

What has been the budgetary impact for MSPs and service providers post COVID-19?
Only 37.5 per cent of service providers report no impact on their operational budget due to COVID-19. The remainder have a budget impact or believe it is still too early to determine budget impact. For those with budget impacts, the lower end of the scale is between 10 per cent to 19 per cent negative impact with the upper end at 40-49 per cent.

JOB ADVERTISEMENT ANALYSIS

Only 1 in 4 service providers have an internship program.

Service Providers found it most difficult to attract and retain people with skills in:

Strategy | **Risk & Governance** | **Compliance** | **Consultancy**

Slightly less than 1,000 cyber security positions were advertised online via job advertising website Seek across Australia during the study, with 484 positions advertised in May and 508 in June. New South Wales accounted for 142 of those in May and 189 in June indicating a steady increase, however a longer analysis period is required to indicate key trends. These numbers represent between a tripling to quadrupling in the number of cyber security jobs advertised as compared to an equivalent time period four years ago. The number of cyber security jobs advertised in NSW is approximately 63 per cent more than is available in Victoria. This indicates either rapid growth in NSW cyber security, a higher turnover of roles in NSW, a dramatic slowdown in cyber security jobs in Victoria or a combination of the first two with a slowing Victoria.

The online job search website Seek (www.seek.com.au) was selected as the focal platform for this research, as it is one of the most popular job searching websites in Australia. However, it is worth noting that many positions, particularly more senior positions, are unlikely to be advertised on an online site such as Seek. Accordingly, the results should not be taken to indicate a comprehensive picture of cyber security jobs available in Australia over the relevant period. However, the results can be used to show trends and information about characteristics attaching to typical cyber security job vacancies (including salary, experience requirements and location).

Within the study, job roles were selected based on the advertisements and text search analysis to determine key job types.

METHODOLOGY: MEMBER SURVEY, JOB ADVERT ANALYSIS & CISO SURVEY

A series of initial interviews with the main stakeholders was undertaken to help establish the key questions to be investigated as part of this research. Following those interviews, AISA surveyed its 6,500+ individual and corporate members based on the interview findings and issues identified. Separately, 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 and 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.

DEFINITIONS

The terms 'cyber security' and 'cyber security skills' are very broad. 'Cyber security' has been defined as: 'the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation. It is this broad sense of 'cyber security' that is used in this research. In this research, the terms 'cyber security' and 'information security' are used interchangeably.

The term 'skills shortage' could be regarded as analogous to the more generally descriptive term of a 'tight labour market.' It has been proposed that labour market tightness be taken to describe the balance between the demand for, and the supply of, labour. If the demand for labour increases relative to supply, the labour market tightens, then we can expect some upward pressure on the real price of a given quantity of labour.[1]

It has been suggested that the cyber security skills shortage should be defined as the difficulty of finding and retaining appropriately qualified individuals at what are considered reasonable wages.[2] This definition is supported by the 'skills shortage' literature and is consistent with effective demand projections of skills used in the literature.[3]
This study will adopt this definition of cyber security skills shortage.

1. Brigden, A. and J. Thomas (2003). What does economic theory tell us about labour market tightness? Working paper no. 185. Bank of England.
2. Mar tin C. Libicki, David Senty and Julia Pollock, National Security Research Division, The RAND Corporation, (2014) 'H4acker5 Wanted. An Examination of the Cybersecurity Labor Market,' x.
3. Zhang, T., et al. (2014). Skills gaps estimates for institutional and individual decision making: A progress report, Office of Workforce Information and Performance, Division of Workforce Development & Adult Learning, Maryland Department of Labour, Licensing and Regulation.

AISA

As a nationally recognised not-for-profit organisation and charity, the Australian Information Security Association (AISA) champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. Established in 1999, AISA has become the recognised authority on information security in Australia with a membership of over 6,900 individuals across the country. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia.

AISA's vision is a world where all people, businesses and governments are educated about the risks and dangers of cyber-attack and data theft, and to enable them to take all reasonable precautions to protect themselves. As an independent non-profit association, AISA was created to provide leadership for the development, promotion, and improvement of our profession. Our strategic plan calls for continued work in the areas of advocacy, diversity, education, and organisational excellence.

ABOUT THE RESEARCHERS

Professor Matthew Warren is currently the Director of the RMIT University Centre for Cyber Security Research and Innovation. Matthew is a prolific and passionate researcher in the areas of Cyber Security and has authored and co-authored over 300 books, book chapters, journal papers and conference papers. As well as academic research, he is experienced in working with government in advisory capacities and being an external cyber security consultant for numerous international and Australian organisations. Professor Warren has taught in Australia, Finland, Hong Kong and the United Kingdom and is also AISA's Cloud Branch Executive.

Damien Manuel is the Director of Deakin's Centre for Cyber Research & Innovation (CSRI) and Chairman of AISA. A former Chief Information Security Officer (CISO), Damien has also worked as a senior information security governance manager and later as an enterprise IT and security risk manager at National Australia Bank (NAB), where he was responsible for managing the bank's information security standard globally. He also held senior roles at RSA, Telstra and Melbourne IT and is currently on CompTIA's Executive Advisory Committee. Damien has been in the industry for over 28 years and has contributed to the development of global industry certifications for the last 17 years.

AISA

www.aisa.org.au