AISA

Australian Information Security Association

THE AUSTRALIAN CYBER SECURITY SKILLS SHORTAGE STUDY 2016

AISA RESEARCH REPORT

National Australia Bank

TELSTRA

defence science institute

Creating Defence Science Research Networks for Australia

AMSIIntern

DRIVING INDUSTRY & UNIVERSITY COLLABORATIONS

Foreword

Part of AISA's mission is provide advice and guidance to government on the creation of policy, law and legislation in relation to cyber security in Australia. This research into the Australian cyber security skills shortage commenced in May 2016. The aim was to provide support for and help identify solutions that build Australia's cyber security capacity and capabilities.

We believe this research sheds a unique light on the complex issues that underlie the Australian cyber security skills shortage. Rather than a simple case of demand exceeding supply of cyber security workers, this research identifies that the Australian skills shortage is more about organisations that fail to resource appropriately in order to secure their information assets. It is further fuelled by a lack of management understanding of information security risks and exacerbated by limited opportunities for those looking to enter the cyber security area, with the focus by employers and recruiters on prior experience and detailed knowledge of very narrow and specific areas unnecessarily narrowing the pool of available candidates. The reluctance of many employer organisations to invest in development of entry level cyber security workers is a particular concern, raising questions about the career prospects of graduates from vocational and tertiary courses. The profession itself often fails to recognise that, for many, information security is an additional duty to other tasks rather than a full time focus. The research also suggests there is a need for generalists to gain access to appropriate cyber security education, training and support.

Based on the findings from this research AISA is pursuing a number of important initiatives:

- Publication of a **Cyber Security Careers Guide** that identifies roles and pathways for those interested in pursuing a cyber security career;
- Mapping education and training offered by vocational and tertiary education providers and training organisations to cyber security roles and promoting opportunities to members;
- Working with employers to increase their understanding of the need to invest in and grow Australia's cyber security capability; and
- Working with the Australian Professional Standards Council to bring Cyber Security as a profession under the scheme.

The cyber security skills shortage is a topic that clearly resonates with AISA members who have generously contributed to interviews, survey responses and online discussions as part of this research and who have reviewed and analysed the results in subsequent focus groups. We thank them for their support.

Mr Arno Brok

CEO, AISA

Arno.brok@aisa.org.au

October, 2016

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 in Australia.

www.aisa.org.au

Australian Information Security Association
ABN 181 719 35 959
Level 8, 65 York Street, Sydney NSW 2000

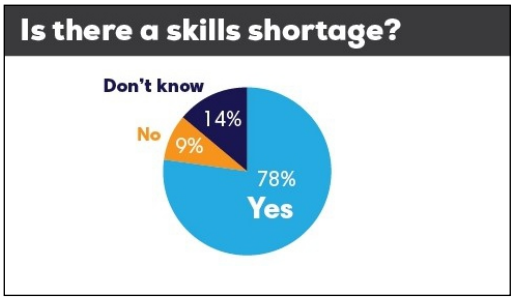
Contents

Table of Figures

Cyber security skills shortage research[1]

Executive Overview

Nearly 78% of AISA survey respondents agree or strongly agree that there is a shortage of qualified cyber security workers for available positions in Australia.



But what does this really mean?

Further analysis suggests that the cyber security skills shortage in Australia may be better characterised as concern about ensuring future capacity, of developing and maintaining a strong pipeline of appropriately skilled cyber security workers to meet the future needs of Australian organisations of all sizes, rather than a current state of chronic shortage of supply versus demand.

Member feedback and other findings suggest that many entities do not appreciate the need forsecurity capability. Other entities, who are unable to find professionals with the skills required,are electing to either leave positions vacant or fill them with more junior or less skilled staff. As a result, it is likely that many organisations are putting the security of their data and systems at serious risk.

Some members saw this as a consequence of the Australian cyber security skills market being comparatively immature.

> *I have worked in the US and Europe for over 15 years and the Chief Security Officer reports to the CFO or board. Most Australian organisations are still operating as if it's the 1990's with a CISO reporting to the CIO. This is your problem, unless that is fixed security will never be taken seriously!*
>
> *AISA Member Comment*

The shortage of cyber security workers in Australia may become an increasingly urgent issue as organisations look to increase their cyber security capacity and capabilities over the coming years.

It remains to be seen whether, in response to limited availability of appropriately skilled workers at an acceptable price, organisations will choose to invest in developing and retaining suitably skilled staff or turn to contractors, consultancy organisations and outsourced service providers for the specialised security skills they require.

> *'The cyber security industry is going to (continue to) evolve rapidly over the coming years, automation will replace some job types, new technologies and, business culture will demand more of generalist and business facing skillsets. Mature cybersecurity professionals will need to adapt, and organisations /government/education industry will need to better prioritise technical and professional development curriculums for younger and mature age professionals.'*
>
> *AISA Member Comment*

[1]*This research has been led by Dr Jodie Siganto, Director, AISA Cyber Security Academy, with support from Professor Matt Warren, and DrRuwanSeranathan from Department of Information Systems and Business Analytics, Deakin Business School, Deakin University whose engagement was organised through the AMSIIntern program with financial contribution by the Defence Science Institute. Otherfunding for this project was provided by Telstra and National Australia Bank. AISA is very grateful for their support.*

For many, this is an opportunity for Australian cyber security workers to get ahead of the curve, provided they are agile and able to adapt to a rapidly changing environment.

'This is a pervasive and holistic issue. Australia is on the cusp of a digital revolution that has already hit the rest of the world. As the world changes and everything is connected and integrated, our preparedness as a nation will place the economy at extreme risk. Without the people with skills to address these risks, we are doomed to failure.'

AISA Member Comment

Key Findings

Is there a shortage? A large majority (78%) of members believe there is a cyber security skills shortage in Australia.

Salaries and turnover rates: Information provided in relation to salaries and job turnover (traditional indicators of a labour market shortage) suggest that both remain relatively stable. Job postings indicate that cyber security workers are paid somewhere between the average adult fulltime wage for more junior roles (such as security analyst) and up to 2.5 times the average wage for managers and other senior positions. [2] This is consistent with the member view that they were being reasonably well paid.

By cross referencing pay increases to industry sectors, there is some evidence that those working in industries with the highest shortages (e.g. government, community services and healthcare) were not as well remunerated. A number of respondents, particularly from government positions, noted that many organisations were not prepared to pay the salaries required to secure appropriately qualified staff.

Growth in cyber security teams: Cyber security teams are generally not expanding in large numbers. Fifty-two per cent of respondents reported that their team had remained about the same or grown by less than 10% while over 11% of respondents reported a decrease in size.

How concerned are you about the Australian cyber security shortage?

The cyber security skills shortage is not an issue of serious concern to most respondents. Seventy per centare either 'somewhat' or 'quite' concerned. Only 16% were 'very concerned,' while 14% weren't concerned at all.

THE AUSTRALIAN CYBER SECURITY WORKER

What does the average AISA member look like?

- Male
- Aged 35 – 65
- 10-years cyber security experience
- Bachelor degree or higher
- CISSP, CISA/CISM
- Full-time employee
- Likely to work for a large organisation - most likely a bank, government agency or consultancy firm
- Based in Sydney, Melbourne or Brisbane
- More likely to be involved in a security management role than a technical role.

Reasons for Skills Shortage: Management lack of understanding of skills required was given as the main reason for the Australian cyber security shortage, followed by an insufficient number of appropriately skilled people for available positions and employers' reluctance to recruit and train entry level candidates. Each of these reasons were important themes re-iterated by many members in their accompanying comments

What do you think are the main factors contributing to the Australian cyber security skills shortage?

The importance of experience: 90% of advertised cyber security positions (including junior positions such as security analysts) required a minimum of five years' experience.

Most respondents agreed that experience was the most important criteria for organisations looking to recruit cyber security workers although certifications were also regarded as a significant indicator of skills. In the job postings, the CISSP certification was the most commonly included criterion (Note: The CISSP requires 5 years' experience). Many respondents did not think that current academic qualifications adequately prepared cyber security graduates for the workplace. Where are the new cyber security workers coming from?

The average Australian cyber security worker is 36 or older. But where are the new entrants? Only 42% of employers recruit entry level candidates. Members believe that one of the major contributors to the shortage is employers' reluctance to recruit and train entry level candidates. This needs to be addressed. Perhaps of most concern was the finding that close to 50% of the employer organisations do not take entry level applicants. This finding raises questions about how easy it is for people with no prior experience looking to enter the cyber security workforce.

Where are the new cyber security workers coming from?

The average Australian cyber security worker is 36 or older. But where are the new entrants? Only 42% of employers recruit entry level candidates.Members believe thatone of the major contributors to the shortage is employers' reluctance to recruit and train entry level candidates. This needs to be addressed.

Shortage in technical roles: Members believe shortages are mostly in technical roles: architects, forensics examiners and incident handlers. The focus on technical positions is consistent with the analysis of online job postings, which identified roles such as security analysts, technical consultants and architects as most in demand. A number of members commented that many employers and recruiters had impossibly high expectations of the range of skills and experience required by successful candidates for particular jobs.

Sector specific shortages: Currently, the largest employers are financial services entities, federal government agencies and consulting organisations. Perhaps not surprisingly, consulting organisations were among the biggest recruiters according to the online postings, followed by government and finance service providers. However, these industry sectors were not ranked highly by members as sectors with skills shortages. This perhaps reflects the view that it is those areas with the lowest existing security capabilities that have the biggest skills shortage.

[3]The average adult weekly wage at May 2016 is $1,573, or $81,796 p.a. based on information from the Australian Bureau of Statistics. http://www.abs.gov.au/ausstats/abs@.nsf/mf/6302.0

Is the cyber security skills shortage a bigger problem for smaller organisations?

Where are the shortages? Another area where member opinion and the job posting analysis differed was the geographies in which shortages were most acute. Members believed that security skills shortages were more prominent in regional areas, Perth, Darwin, Hobart and Adelaide. However, no positions were advertised in Darwin, Hobart or regional areas over the period of analysis, with most advertised jobs being in Melbourne, followed by Sydney and Brisbane.

Contractors vs fulltime positions: About 20% of the advertised positions were for contractors rather than fulltime employees. This relatively high number suggests that employers may be unwilling to invest in building long-term internal cyber security capability and are increasingly relying on the skills of contractors, consultants and outsourced service providers. This proposition is further supported by the relatively high number of members who work in consulting firms, professional services organisations and vendors.

Role Clarity: Seventy-eight per cent of members believed that lack of clarity about skills required for different job roles contributes to difficulties in recruiting for cyber security roles.

Finding the Unicorn

'Employers are looking for mythical unicorns. Employers want a pen-tester with scripting abilities, web application knowledge, listed CVE's, who has presented at a conference, can make coffee, plays sports and has written his own tools in his spare time. This said person should have good command of English and strong business acumen. The mythical unicorn doesn't exist.'

AISA Member Comment

What this means for AISA

There are some clear messages and actions for AISA from the results of this research, many of which are already well underway. Key takeaways for AISA include:

	Issue	AISA Response
Raise importance of cyber security	AISA must engage more closely with all Australian organisations to help them understand the importance of having access to appropriately skilled cyber security workers. Particular focus will be on those organisations who may not currently appreciate the importance of information security.	This is a key commitment of the AISA Board and CEO.
Engage with employers and recruiters	AISA must engage more closely with Australian employers and recruiters to increase their understanding of different cyber security roles and relevant skills and competency requirements and to consider more flexible work options for cyber security employees.	AISA will progress the publication of an **Australian Cyber Security Careers Guide** directed at employers and recruiters. The **Careers Guide** will explain different security roles and associated skills and competencies and also provide background on existing industry and vendor certifications and relevant academic qualifications.
Develop new breed of cyber security workers	The professional development of most information security professionalsis directed at fulltime employees of existing organisations.	AISA is looking at diversifying the skills base of information security professionals & equipping them for the new paradigm of operation.
Introduce professionalisation scheme	Employers should have some reference guide or system to confirm the skills and competencies of information security professionals.	AISA is working on the development of a professionalisation program which will include the accreditation of information security professionals.
Identify cyber security career paths	Career paths for people interested in pursuing a career in information security must be clearly identified and relevant information and guidance material made widely available.	AISA will progress the publication of an AISA **Cyber Security Careers Guide**.
Develop transition paths	Transition paths for mature workers into the information security industry need to be identified and made known.	Identifying and supporting transition paths is a key objective of the AISA Cyber Security Academy and will be included in the AISA **Cyber Security Careers Guide**.

	Issue	AISA Response
Increase entry level employment opportunities	More organisations should provide employment opportunities for new entrants to the cyber security field.	AISA will pursue this through its support for a wide-range of education and training initiatives via the AISA Cyber Security Academy as well as engagement with its members.
Support continual education of cyber security professional	Information security professionals must continually improve their knowledge and skills (including their soft skills) to keep pace with the rapidly changing environment.	Continuing improvement of cyber security works skills and capabilities will be addressed by professional development programs offered by the AISA Cyber Security Academy.
Support the development of soft skills	Soft skills, such as negotiation and leadership, are important to the success of cyber security workers.	The AISA Cyber Security Academy will provide opportunities for the development of relevant soft skills.
Educate and train generalists	IT generalists, who are not 100% focused on security but provide a wide-range of services to Australia's small and medium organisations, must have the opportunity to acquire relevant cyber security skills.	The AISA Cyber Security Academy will provide access to a wide range of education and training options. This is one of the key initiatives being pursued by AISA.
Provide solutions for SMEs	Solutions for ensuring SMEs are able to access appropriate security advice and services must be developed.	AISA will establish a communications network with other bodies likely to influence SMEs and with government agencies who are also working in this space. In addition, further research will be undertaken to help AISA understand the security requirements of Australia's SMEs and how those requirements may best be met.
Increase cyber security skills of whole community	The cyber security skills of all Australians must be increased and maintained.	AISA is targeting greater community outreach and engagement.

Methodology: Member survey, job ad analysis and focus group discussions

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 members based on the interview findings and issues identified from a literature review. Separately, details of positions requiring information security skills advertised in Australia on Seek.com between May and July 2016 were collated.

All of this data were analysed and the initial findings included in a draft report which was then tabled for discussion with a range of different stakeholders and in focus group sessions. Feedback from those sessions was included in this final report.

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.[3] 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.[4]

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.[5] This definition is supported by the 'skills shortage' literature and is consistent with effective demand projections of skills used in the literature.[6]

This research will adopt this definition of cyber security skills shortage.

[3]U.S. Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies, https://niccs.us-cert.gov/glossary#letter_c

[4]Brigden, A. and J. Thomas (2003). What does economic theory tell us about labour market tightness? Working paper no. 185. Bank of England.

[5]Martin 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.

[6]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 Labor, Licensing and Regulation.

AISA survey findings

Methodology

AISA members were asked to complete an online survey on issues relevant to the Australian cyber security skills shortage, identified from a review of the literature dealing with the cyber security skills shortage both globally and as it affected Australia[7] and on interviews with initial stakeholders. The survey was open for approximately three weeks in July 2016. Over 400 individual AISA Members completed all or some part of the survey.

As part of the survey, participants were given the opportunity to provide any other thoughts or comments that they might have in regard to the cyber security skills shortage. Over 134 participants took the opportunity to share their additional views. Most of the volunteered commentary related to where responsibility lies for the cyber security skills shortage.

The following findings are based on analysis of the responses to that survey and the additional comments provided by the survey respondents and also includes some findings from the job postings analysis included in the next section of this report.

Survey findings

Do members think there is a cyber security skills shortage?

Members were asked to indicate the extent to which they agreed with the proposition that there is a shortage of qualified cyber security workers for available positions in Australia.

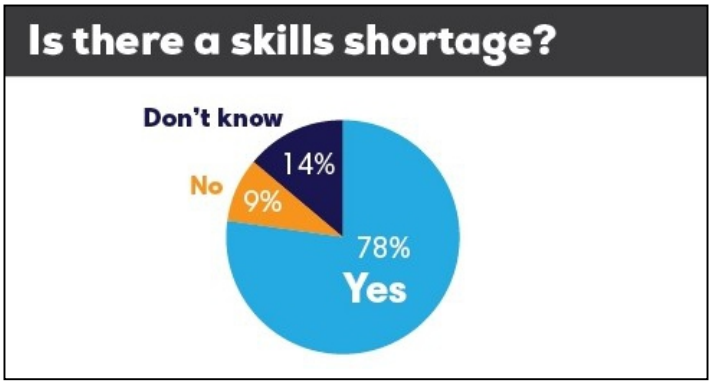


Figure 1: Do you think there is a shortage of qualified cyber security workers?

A large majority of members – 78% in total - believe there is a cyber security skills shortage in Australia.

[7] A detailed Literature Review Report is available from AISA on request.

A number of members included comments about this issue, some supporting the existence of a skills shortage and others taking the contrary view. One member replied that he knew there was a skills shortage and that this survey was the 'worst ever' as it gave those who didn't know an opportunity to provide their opinion. Others challenged the existence ofan Australian skills shortage:

> *'There is no Skills shortage in Australia for Cyber Security. People are not getting jobs, no interview calls ... how can you even start this survey !!!!!'*

> *'There is no skill shortage. When advertising an average of 15+ CVs are received.'*

Notwithstanding that a high number of respondents agree that there is a cyber security shortage, the issue is not one of serious concern. Asked to indicate their level of concern, 70% indicated that they were either 'somewhat' or 'quite' concerned.

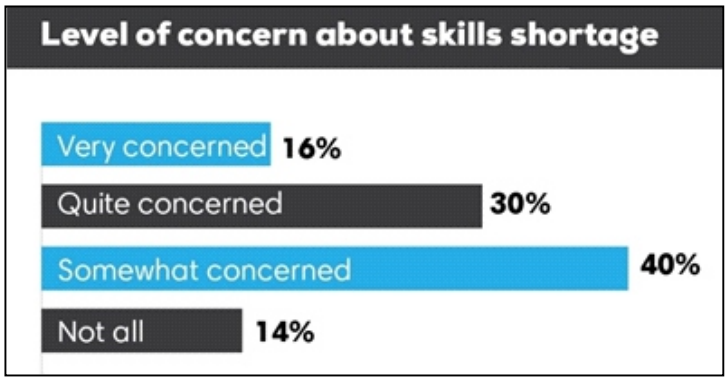


Figure 2: Level of concern regarding cyber security skills shortage

This lack of strong concern may indicate a pragmatic view by members:

> *'if it is real, at least ill always have a job :).'*

> *'Demand and supply will eventually balance out. In the meantime, security experts enjoy great job security and big wages.'*

Despite members being very clear that they believed there were not enough cyber security workers for available positions, there was considerable commentary by members to the effect that the cyber security skills shortage was more a failure by organisations to recruit or retain an appropriate number of cyber security workers. This view puts the skills shortage in a different context perhaps outside the traditional view of a shortage of supply versus demand. This alternative view casts the skills shortage as a failure to recruit, more than a failure of supply:

> *'This survey does not acknowledge that not only is there a skills shortage; there are also role shortages in every organisation in Australia. Companies are still not putting a large enough priority on security as a whole, and therefore the business and HR are not creating enough roles within their organisation dedicated to protect the business from attack.'*

> *'There is not enough awareness that it's a critical business function and needs to be resourced accordingly.*

> *'I would suggest that employers are not employing enough cyber security employees at all levels as Cyber Security in Mining is not seen as a significant threat.'*

> *'In general, the companies are only just starting to wake up to the risks and obligations. They do not understand the scope and therefore do not know who or what skill sets they need to acquire.'*

The proposition that the cyber security skills shortage may be an organisational failure to recognise the importance of security and resource accordingly is supported by other findings in this research, including the finding that members believe that 'management lack of understanding of skills required' was the biggest factor contributing to the skills shortage.

Factors contributing to the cyber security skills shortage

Respondents were asked to indicate the top three factors which they believe contribute to the cyber security skills shortage in Australia, choosing from a list of options but also with the opportunity to specify other factors and to provide further comments.

Factors contributing to the skills shortage	Response
Management lack of understanding of skills required	64%
Insufficient appropriately skilled people for available positions	57%
Employers reluctance to recruit and train entry level candidates	51%
Employers failure to offer appropriate salaries	40%
Failure to high light cyber security as a career option in schools	40%
Insufficient or inadequate tertiary cyber security courses	31%
Lack of uptake of STEM subjects in school	22%
Hiring freezes	20%
Need for security clearances and other delays in recruitment process	20%
Over emphasis by employers on experience	20%
Lack of diversity in the workforce	11%
Lack of flexible working arrangements	10%

Figure 3: Factors contributing to skills shortage

The selection of 'management lack of understanding of skills required' as the biggest factor contributing to the skills shortage supports the characterisation of the cyber security skills shortage as at least in part an organisational failure.

A number of members commented on management's lack of understanding of the skills required:

> 'I think that the business is the reason cybersecurity suffers. It appears that many organisations are not proactive but rather reactive when it comes to cybersecurity breaches. With this in mind it becomes difficult to appreciate the costs associated with investing in the skills that can protect an organisation as a whole. At best an organisation may have an engineer that patches and manages a firewall.'

> 'The vast majority of businesses that I've worked with – either through consultancy or when I held senior management positions for some nationals and internationals – just don't care enough about risk and security to fund the roles.'

In terms of the other main reasons for the skills shortage, a number of members referred to the absence of a clear career path for people interested in pursuing a cyber security career:

> 'Although there seem to be a number of low-paying lower-skill roles often on offer, there is no clear career path or way to enhance skills further except in a select few areas. So people move on to other areas before they get the experience that recruiters seem to want to see for more advanced roles.'

> 'The shortage is there because they don't want to pay more and there's no career path to senior management in most organisations.'

Stability of salaries and employment

Quickly rising salaries and a high turnover of staff are indicators of a market where demand exceeds supply, that is, where there is a labour shortage. Respondents were asked a series of questions to determine whether either of these indicators were present in the Australian cyber security work force.

A strong majority of the respondents rejected the traditional definition of a labour shortage, disagreeing with the proposition that stable salaries and low turnover in jobs indicate that there is no cyber security skills shortage. Although strongly of the view that there is a skills shortage,information provided by respondents suggests that their salaries are stable, with minimal increases over the previous 12 months, and that a majority of respondents have been in their current position for at least 2 years, indicating a low churn rate.

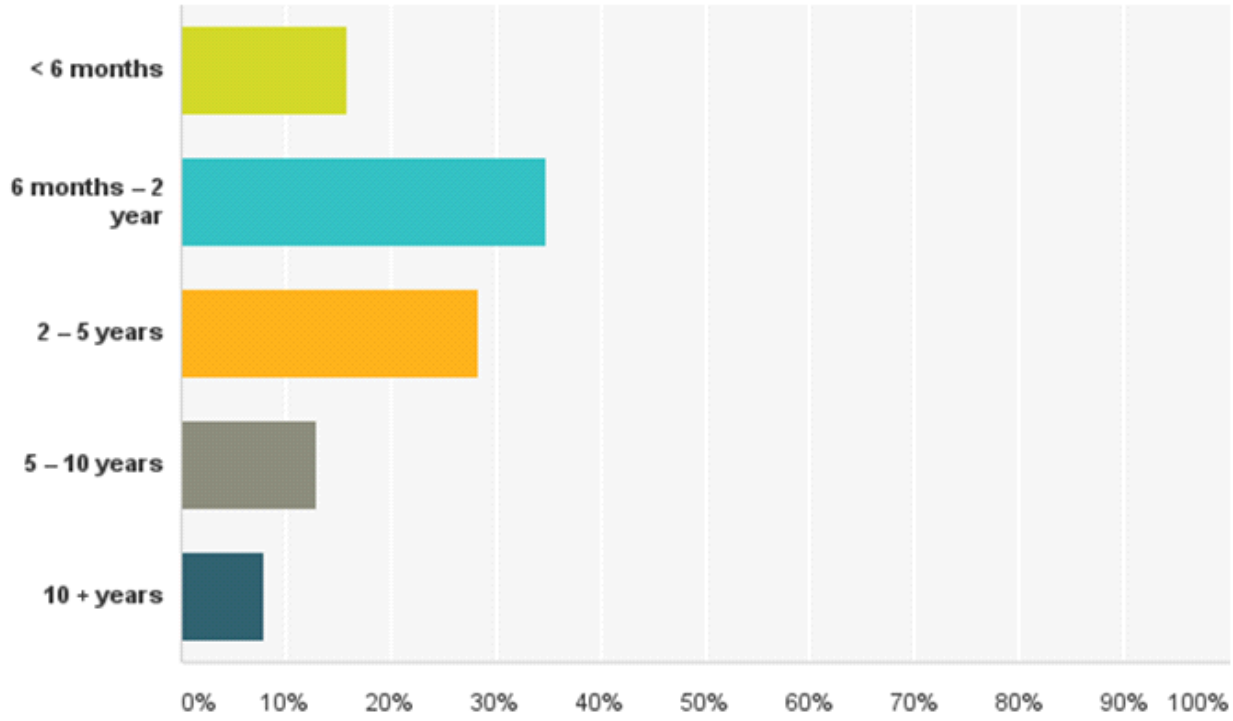


Figure 4: How long have you been in your current position?

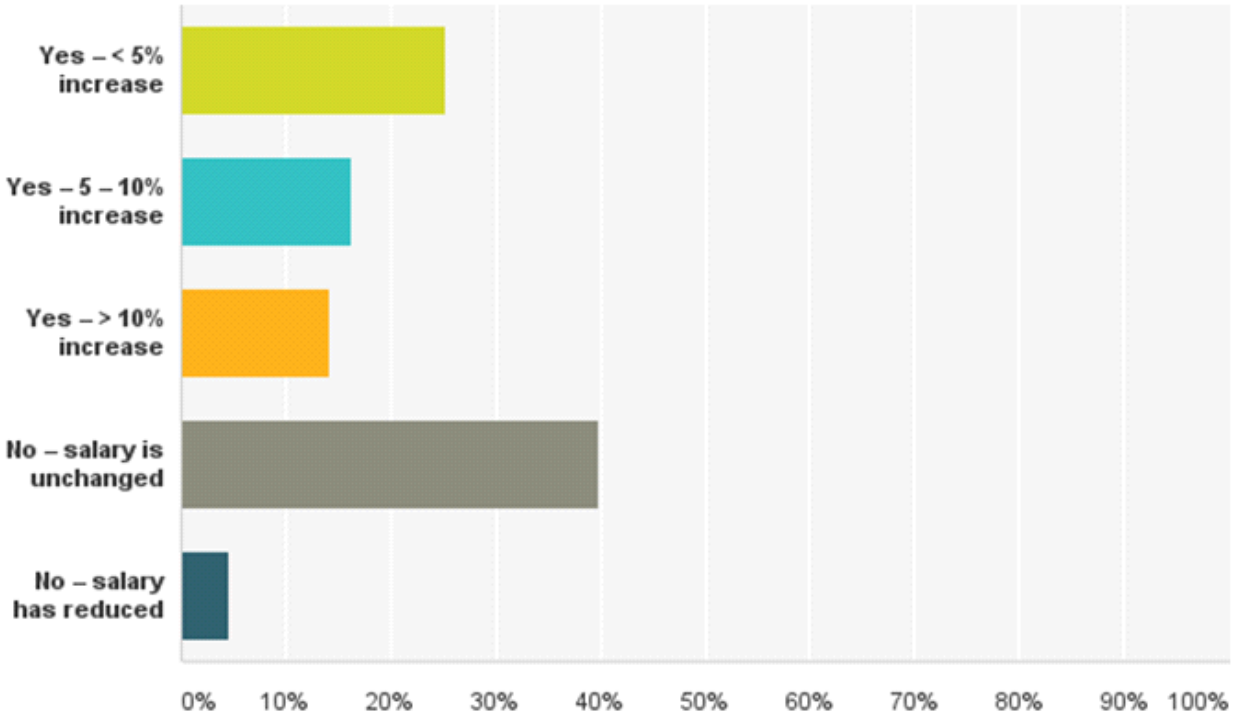


Figure 5: Have you received a salary increase in the last 12 months?

Although close to70% of respondents had either a reduction in salary, no salary increase or an increase of less than 5%, 36% of respondents believed their salaries were increasing more than average. Thirty-two per cent thought they were not keeping pace and 32% didn't know.

By reference to the advertised salaries for cyber security roles, the salaries paid to cyber security workers seem generally to be rising consistently with those paid to workers in other areas. A spokesperson for a large international recruitment consultancy confirmed that salary growth in Australia has been around 3% per year and that not many groups are being paid in excess of that. This seems to be consistent with the salary rises reported across the board for Australian cyber security workers.

Job postings also indicate that cyber security workers are paid somewhere between the average adult fulltime wage for more junior roles (such as security analyst) and up to 2.5 times the average wage for managers and other senior positions. [8] Salary ranges based on information included in advertised cyber security rob roles are included in the figure below.

Job Role	Salary range	
Analyst	$70k	$150k
Consultant	$80k	$170k
Manager	$100k	$230k [9]
Architect	$100k	$270k [10]
Engineer	$120k	$145k
Director, Owner or CEO	$180k	$220k

Figure 6: Range of salary for job roles

Interestingly the salary ranges for each job role differed between capital cities. Melbourne reported the highest pay rate for analysts and architects, with Sydney also offering higher pay rates for architects (see the figure below). This may reflect the predominance of financial service institutions in those cities which anecdotally at least are believed to offer higher salaries than other industry sectors.

	Sydney	Canberra (ACT)	Melbourne	Brisbane	Adelaide
Analyst	80k - 150k	70k - 110k	200k+	-	85k - 90k
Consultant	80k - 170k	-	100k - 150k	150k - 165k	-
Manager	100k - 200k	230k	130k - 150k	-	-
Engineer	120k - 145k	-	130k+	-	-
Architect	100k - 270k	130k - 150k	200k - 270k	-	-
Director, Owner or CEO	-	-	180k - 220k	-	-

Figure 7: Range of salary for job roles in different cities

[8] The average adult weekly wage at May 2016 is $1,573, or $81,796 p.a. based on information from the Australian Bureau of Statistics. http://www.abs.gov.au/ausstats/abs@.nsf/mf/6302.0

[9] The $230,000 Melbourne job was for an APAC team manager and was based on full on-target earnings, that is, including discretionary elements like bonuses.

[10] The $270,000 architect job was for a senior architect to lead a team in a large consulting practice.

Summarising these results, most of the respondents believe there is a cyber security skills shortage in Australia while the traditional economic indicators of labour shortage suggest the contrary. Salaries are largely stable, cyber security workers generally believe they are being reasonably well paid and salary rates would indicate that this is the case. There is also no evidence of high staff turnover.

There may be other explanations as to why there is no evidence of upwards pressure on salaries, which might be expected if there was a traditional skills shortage. It is clear that there is some reluctance to pay security people what some think of as 'appropriate' salaries. One commentator said that rather than a cyber security skills shortage, there is 'a shortage of budget to pay people what you need to pay them to attract them, and to attract people in other industries.[11] Many respondents commented to that effect:

> *'I've watched organisations that are struggling to fill positions with quality candidates, yet they are unprepared to pay enough to get quality candidates.'*

> *'There is no cyber security skills shortage however, there is a shortage of adequate funding to attract/retain suitable cyber security staff! If the employers won't or can't get the money, then they won't get the staff - there is no shortage of staff.'*

It seems that employers not able to fill advertised positions (whether because of the salary offered or the availability of staff) may either leave them vacant or recruit candidates who do not have the desired experience or qualifications. This in turn would reduce the upwards pressure on salaries. There were a number of comments that supported this as an option.

> *'In the last five years federal Government has lost more than 50% of its cyber security work force to industry. The skills shortage is dire. Many have been snapped up by industry with only two years' experience in entry level/graduate cyber security roles. Others have been at senior levels with five or more years' experience. The loss of staff has not been replenished and month on month more people are leaving the Government sector cyber security roles than joining. Those that are joining would be 80-90% junior entry or with minimal experience.'*

Difficulties in recruiting because of wage restrictions and the tendency to leave positions unfilled are consistent with evidence of the limited growth of cyber security teams. Fifty-two per cent reported that their team had remained about the same or grown by less than 10% while over 11% of respondents reported a decrease in size. Just over a third of the respondents (36.5%) indicated that their team had grown by more than 10% during the term of their employment.

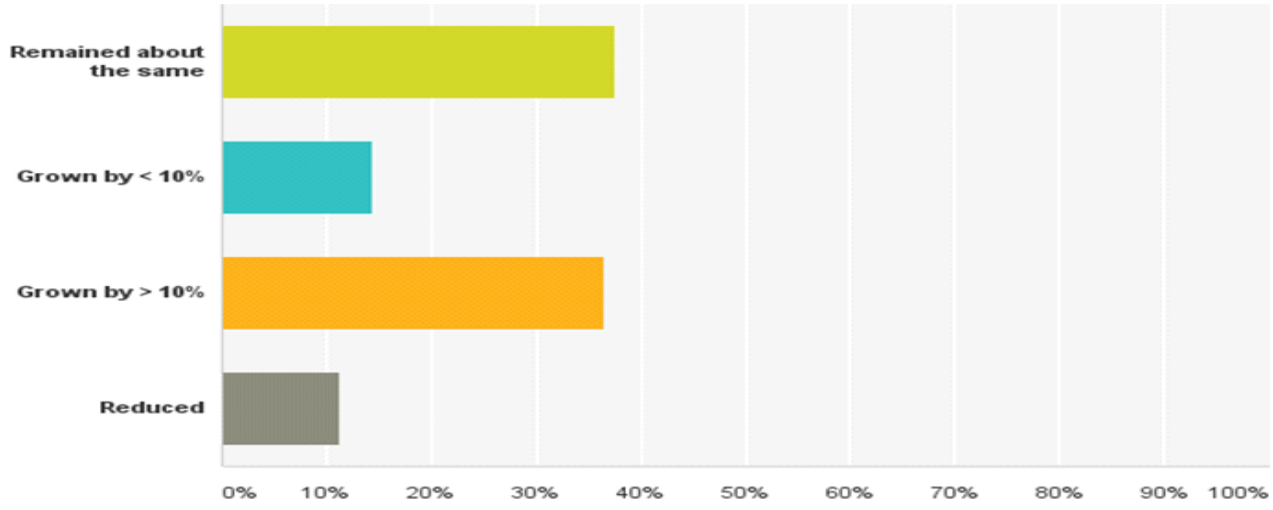


Figure 8: Growth in your employer's security workforce during your employment

[11]Gothard, P. (2015) Cyber security skills gap: 'Pay more and the problem will go away,' says Reuters IT security chief.

What does the skills shortage look like?

Roles

Members who believed there was a skills shortage were asked to indicate all the roles where shortages applied. The top roles selected by members as being affected by the skills shortage were architects and technical security consultants.

Figure 9: Roles with shortages of qualified cyber security workers

These findings are largely consistent with the job postings analysis discussed below which indicate that the following were the most advertised positions: analyst, consultant, manager, engineer and architect. Of these, the cyber security analyst was in highest demand.

Business continuity manager, developer, network administrator, information assurance manager, trainer and privacy officer were all roles where members did not believe there was a significant skills shortage.

It is of interest to compare roles members believed may be in short supply to those regarded as important by Australian CIOs. According to recent research, Australian CIOs believe cloud security (54%), hacking and penetration testing (38%), big data and data analytics (32%) and IT security technologies (32%) are the top technical security skills in demand.[12]

Experience vs qualifications

There is some debate in the literature over the importance of experience (and the assumed acquisition of skills and capability) versus knowledge which might be gained through completing academic qualifications or certifications from industry bodies such as (ISC)[2], ISACA and SANS or vendors, such as Cisco. Members were asked for their opinion on a series of propositions designed to test the importance of experience versus qualifications when recruiting cyber security workers.

Although not significant, there was a preference in each case for the propositions that:

- Experienced cyber security workers are in short supply; and
- Experience is more important to recruiters than knowledge, certifications or education.

A number of survey respondents referred to recruiters' preference for experience. However, there were also some respondents who took the contrary view; that certifications were given more importance than experience.

'There is a skills shortage. However, it is less about "qualifications" and more about "capability".'

[12]Robert Half, *Cyber-security Defending your future*, September 2016 at 12.

Figure 10: Experience vs certifications vs education

Members also noted that certifications did not necessarily evidence knowledge or skills:

> *'There needs to be some form of skills measurement/demonstration - and not more certifications. They do not confirm skill - they confirm the ability to retain knowledge until at least the exam date - not the ability to apply it in the real world.'*

> *'I have interviewed over a dozen people in the past month, from many diverse backgrounds, where the CV is obviously inflated, or where there is an over emphasis on certifications rather that capability and behaviours.'*

A number of members were critical of the academic qualifications available for cyber security workers. This may be because recruiters and employers do not understand the different academic qualifications that are available and the knowledge and capabilities of the graduates from those program. It may also be because existing academic courses are not appropriate for Australian cyber security workers.

> *'My perception is that in terms of qualifications, security certifications are everything and university courses have limited value.'*

The role of recruiters and their perceived failure to understand the skills and competencies required for different cyber security roles was the subject of a number of comments:

> *'Often times large organisations are guilty of using large generalist recruitment firms &/or their own internal recruitment teams who do not have the knowledge, network or the experience to source the qualified talent that is out there in the broader community.'*

> *'Many security roles I've seen are poorly advertised, resulting in the wrong candidate for the wrong role.'*

> *'The recruiting industry in Australia is a disgrace. They treat people like shit. They trawl for resumes with zerocustomer care. The recruiters have zero idea about technical skills or the practice of security. They damage the security profession and all of IT in general. I would tow all recruiters out to sea. Every. Single. One.'*

One member suggested this problem could be resolved via the development of greater understanding of different cyber security roles and competencies by recruiting agencies.

Another issue raised by members was the difficulty in assessing the skills or competencies of cyber security workers. A number of respondents referred to the difficulties in recruiting cyber security workers who:'claimed achievements that are not able to be evidenced at interview.'

> *'The industry is fragmented and lots of shallow people posturing with professed but not real skills.'*

> *'The standard of professions is very patchy with a lot of very average performers - which has a negative impact on security.'*

Other criticisms included recruiters being too focused on finding candidates with the exact experience or qualifications:

> *'Current recruiting seems to be very blinkered to only people with experience or specific education/training, which means a lot of highly skilled and experienced people who want to get into the industry simply cannot, despite having a lot to offer.'*

> *'Recruiters …filter applications only by searching keywords in the CV. If they don't ding the keywords, they won't forward the CV to employer. It happened with me for almost all positions I applied for.'*

A number of other participants referred to the unrealistic expectations of employers and recruiters in regard to the experience, certifications and qualifications that should be held by job candidates.

Finding the Unicorn

'Employers are looking for mythical unicorns. Employers want a pen-tester with scripting abilities, web application knowledge, listed CVE's, who has presented at a conference, can make coffee, plays sports and has written his own tools in his spare time. This said person should have good command of English and strong business acumen. The mythical unicorn doesn't exist.'

AISA Member Comment

Entry level Vs advanced practitioners

Members were asked to indicate whether they thought shortages were more pronounced in entry level versus advanced positions or across the board.

Cyber security skills shortages:	Respondents who agreed with statement
Are more prominent in entry level positions	8%
Are more prominent in advanced positions	39%
Apply across the board	50%
There are no shortages	3%

Figure 11: Level of cyber security shortage

Although 50% of respondents believed the shortages applied across the board, nearly 40% believed the shortages were more prominent in advanced positions. This is consistent with roles such as architect and forensic examiner, all positions requiring experience, being identified as specific areas of shortage.

The analysis of the job postings indicates that there were very few entry level positions advertised in the relevant period. Even those few that were clearly targeted as junior or entry level applicants expected some sort of prior security experience. An example is an advertisement for a Junior Security Analyst, [13]promoted as:

> Exciting opportunity for a Jnr Security Analyst to grow within a leading company
> … Please note that this is a Junior role & requires someone who is willing to learn & further their career.

The specified requirements for this role included:

- Demonstrated experience in developing IT security standards and procedures
- Experience conducting risk assessments and providing advice regarding information security
- Broad knowledge of the major trends, strategic directions and legislative and governance frameworks relating to information security
- Relevant IT Security qualifications such as CISSP, CISM, etc.
- Self-motivated, results oriented and driven to improve business processes
- Exceptional verbal and written communication skills.

It seems unreasonable to expect that a junior analyst would have the sort of experience listed or hold either a CISSP or a CISM, both of which have extensive prior practical experience requirements as conditions for their award.

The focus on experience in advertised positions and the very few number of advertised entry level positions raises questions about how new people, without relevant prior experience, might enter the information security profession.

Respondents were asked whether their current employer took on entry level cyber security workers e.g. school leavers, TAFE or university graduates, talented hackers. The majority of organisations do not (see figure below).

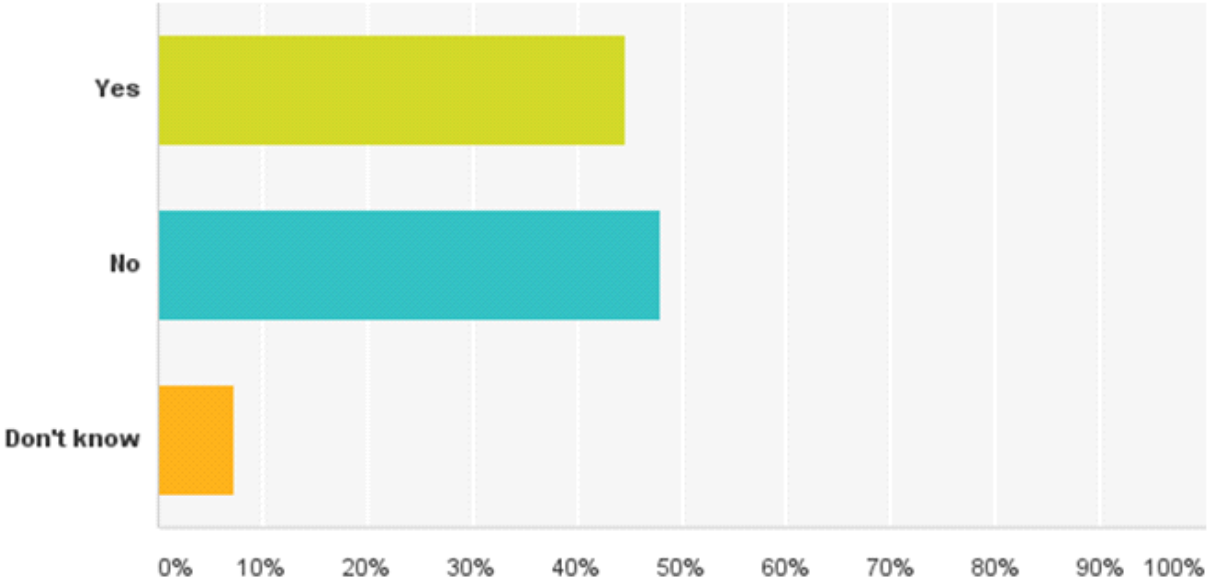


Figure 12.Does your current employer employ entry level cyber security workers?

[13]*Junior Information Security Analyst* Role in Sydney, seek.com.au 23 May 2016.

This finding, that close to 50% of the employer organisations for cyber security workers do not take entry level applicants, is concerning.

It is also an important finding in terms of career paths for cyber security works. If there are few entry level positions and most people come to cyber security after gaining experiencein other complementary areas, then it may be more appropriate to focus on developing career paths for experienced workers from other disciplines who are interested in transitioning to a fulltime cyber security position.

The proposition that cyber security workers rarely start with the intention of pursuing information security as a career and are more likely to transition from other IT roles was identified in the AISA's *Cyber Security Cartographies Downunder* [14] research project. In that research, only one of the 10 Australian information security practitioners interviewed had commenced their careers intending to work in information security. All of the intervieweeshad begun their career with some sort of role relating to information technology including working as computer administrators, network administrators, application developers and other general IT roles. At some stage each had been exposed to security issues raised by a particular project or had interacted with the organisational security team and so had become interested in pursuing a fulltime role in security. Only one had completed a cyber security academic qualification at the graduate level.

The fact that so few organisations employ entry level cyber security workers also suggests that many employers are not prepared to invest in training or upskilling staff to develop the necessary skills and competencies. This reluctance to invest in training entry-level employees may be a consequence of concern that past investment in up-skilling staff has not paid off. This seemed to be a particular issue for those working for government. One respondent noted that he trained people for them to be 'taken away by better salaries in the private sector.'

Internal training of staff seemed to be more than an entry level recruitment issue. A number of members referred to the lack of attention given to the in-house development of cyber security skills (which was also identified in the survey as the third highest reason for the cyber security skills shortage):

> *'Cyber security organisations must demonstrate flexibility and a willingness to recruit, train and support new entrants to the cyber security sector. Industry improvement and growth can only successfully occur from within, so employers need to start investing in people.'*
>
> *'There is lots of attention raised about the skills shortages, but very little encouragement by the sector to attract new recruits. The expectation seems to be that somehow the people will just exist with skills, but entry level jobs aren't on offer in any great way.'*
>
> *'I wonder if organisations want an instant fix rather than to invest in people.'*

Another interpretation of the limited opportunities for entrants to the cyber security work force may be the relatively immature and comparatively small cyber security workforce in Australia. The demand for cyber security workers in Australia may not be sufficient to justify investment in the sort of large graduate recruitment and training programs that are undertaken, particularly by governments, in some overseas locations, which then feed cyber security workers into the private arena.

[14] Cyber Securities Cartographies Downunder is part of the Cyber Security Cartographies project run by the UK Research Institute in Science of Cyber Security (RISC). RISC is one of three Research Institutes formed as part of the UK National Cyber Security Strategy. The CySecCa research team is led by Dr Lizzie Coles-Kemp of the Information Security Group (ISG), Royal Holloway, University of London

Industry Segments

The literature suggests that the cyber security skills shortage may be more acute in particular industry segments, such as government and high tech businesses. There was no clear view from the survey participants on whether the Australian cyber security skills shortage was more acute in any particular industry segment. While 49% agreed with the proposition that cyber security skills shortage was more prominent in some industry sectors than others, 33% of respondents had no view on the question and 18% of respondents did not agree with the proposition.

When asked to identify the particular industry segments where there were shortages, participants focused on government, healthcare, education and utilities. Industry segments that members did not rate so highly included financial services, technology services, consulting and development and telecommunications companies.

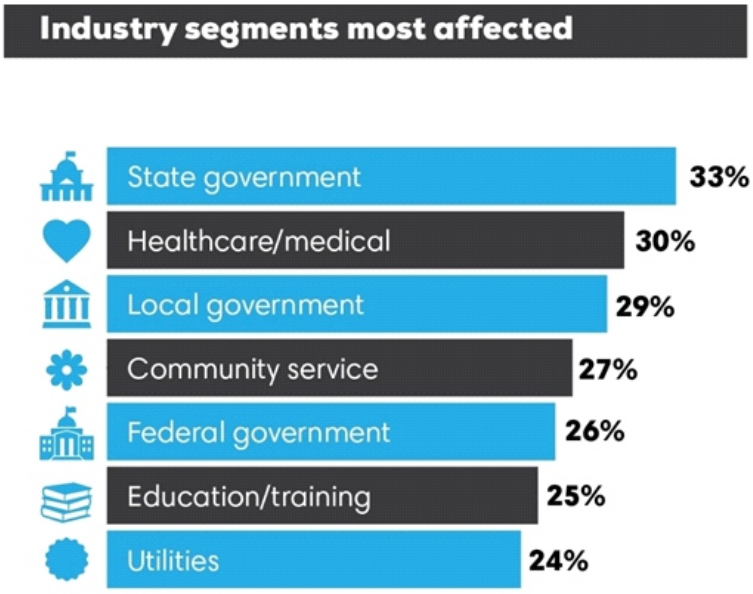


Figure 13: Industry segments most affected by cyber security skills shortages

The identification of state and local government, healthcare and community service providers as industry segments where there are shortages is an interesting finding given that they are not currently large employers of cyber security workers or big advertisers of cyber security roles. Financial service organisations and consulting firms are among the biggest employers of cyber security workers in Australia and were certainly the highest advertisers of cyber security jobs in the period under analysis. However, these industry segments did not rank highly as being affected by the skills shortage.

There is some support for the proposition that larger employers of cyber security workers are less likely to be affected by skills shortages than smaller employers. The literature has referred to the problems faced by smaller employers who do not have the budget or depth of team to be able to recruit and retain highly experienced professionals.[15] Salary certainly seemed to be an issue for many organisations. One of the respondents commented that the salaries paid by the 'Big 4 Banks' had skewed the market for everyone else. This suggests that some large employers are prepared to pay higher salaries to ensure they retain the skills required and fill available positions. By cross referencing pay increases to industry sectors, there is some evidence that those working in industries with the highest shortages according to members (e.g. government, community services and healthcare) were less likely to have received a pay increase of more than 5% and so may not be as well paid as their colleagues working, for example, in the financial services sector or for consulting organisations.

[15]See, e.g. The Rand Corporation (2014). 'H4cker5 wanted. An examination of the Cybersecurity Labour Market', x – xi, '' Caldwell, T. (2013). Plugging the cyber-security skills gap, Computer Fraud & Security: 5-10., UK House of Lords (2015). Make or Break: The UKs Digital Future.

Larger employers (other than government) can also cope with tightening labour markets through internal promotion and education.This position was supported by one of the stakeholders interviewed as part of this research who noted that banks have the luxury of a larger cohort of workers that can be re-deployed as required. This is also consistent with members' opinion that large employers, like those in the financial services industry and consulting organisations, are not so badly affected by the cyber security skills shortage.

Government, and federal government in particular, although a big employer, seems to be impacted by a number of different issueswhich do not affect other large employers. A number of participants commented on the issues facing governments in recruiting and retaining cyber security staff. One of the main issues was salaries:

> *As long as the public sector keeps trying to pay cyber security people the same level as other IT staff, they will keep experiencing shortages. Cyber security entails knowledge of systems, networks, applications, awareness and almost all facets of IT. Appropriate compensation is required for this breadth of knowledge.*

Other factors that impacted government included limitations imposed by pay bands, head count freezes, the need for security clearance and some government departments not having interesting work and perhaps not being regarded as 'cool.' [16]Almost all of the federal government employees who completed the survey said there were shortages in their sector.

> *'It is near impossible to recruit senior cyber security expertise into Government. Graduate, internship and cadetship recruitment remain strongest recruitment sources, but few have cyber security specific skills due to inadequacies of tertiary education sector.'*

However, that view was not shared by respondents who worked for consultancy firms, professional services organisations and vendors. Those respondents rated healthcare, state government, local government and education as the sectors with the greatest shortages, which in turn affected the overall results.

The fact that members see organisations with smaller information security teams (such as those in healthcare, local government and community services) as areas with the highest shortages rather than those with the biggest existing teams and the biggest on-going recruitment requirements is consistent with the view that the skills shortage is more a failure by organisations to make positions available, than of demand exceeding supply. A number of members working in those sectors referred to this problem:

> *"Working in the non for profit health sector, I feel that there is currently little focus on how important cyber security skills are to the industry.'*

Geographical Location of Shortages

Participants were asked the extent to which they agreed with the proposition that the cyber security skills shortage was geographically dependent. Forty-seven per cent of respondents agreed, 14% disagreed and 39% did not know.

When asked to indicate the geographic locations where respondents thought the cyber security skills shortage was most prominent, over 60% of members selected regional areas followed by Perth (52%), Darwin (49%), Adelaide (47%) and Hobart (42%).

This finding was out of step with the geographies where cyber security workers presently work. Based on the postcodes provided for their current work address, almost all of the respondents work in the larger Australian capital cities. Only 15 of the 400+ respondents currently work in a regional area, outside a capital city. However, 60% of respondents identified regional cities as the geographical locations where the cyber security skills shortage is most severe.

[16]Rand, Chapter 3.

Figure 14: Location of survey respondents

It may be that members' opinion is based on the perception that there are unfilled regional cyber security jobs. However, not only are most of the currently filled cyber security jobs in the main Australian capital cities, the analysis of advertised jobs indicates there were no positions advertised outside of the major capital cities in the three-month period during which advertisements were monitored.

One respondent located in a regional area talked about his issues in finding regional employment.

> *'I had been trying to find a job in cyber security for fiveyears. I was constantly knocked back by large firms and small boutique consultancies due to my location. I have now relocated to a capital city and instantly was accepted for a position and offered a few more. I was only a few hundred kilometres away and was happy to commute twice/thrice a week. If there is such a shortage in skills, then why not hire someone to work remotely/commute? Why did I have to move my whole family to find a job?'*

Perhaps the most likely explanation for this gap between what members believe and the evidence of available positions is the contextualisation of the skills shortage by members as a failure by Australian organisations to create the number of roles that should be available, if those organisations properly appreciated the importance of information security.

Defined job roles and competencies

The literature suggests that confusion about job roles and the skills required for particular roles has a negative impact on the ability to recruit appropriately qualified candidates for cyber security roles. Respondents were asked a serious of questions relating to certainty around the skills required for different jobs and the impact that uncertainty might have.

Most respondents agreed that both employers and job seekers are uncertain about what skills are required for different cyber security roles.

Seventy-eight per cent of respondents thought that this lack of clarity makes it difficult for organisations to recruit for cyber security roles. This was confirmed again by the number of respondents who selected 'management lack of understanding of skills required' as the main factor contributing to the cyber security skills shortage (which is

discussed further in the next section).

There is a clear need from the perspective of all participants in the cyber security working space for some definition of different cyber security job roles, and the expected skills and competencies for people holding those roles. This is an action that AISA can undertake.

Generalists

The survey focused on full time cyber security workers, causing a number of respondents to point out that information security practice needs generalists as well as highly skilled specialists, particularly where providing services to small and medium sized organisations. These respondents also made clear that efforts should be made to ensure that those who had security as part of their role received the appropriate support.

> *'For medium sized companies (not banks or gov.) diversity/versatility of skills is also required - not just specialist roles.'*

Another view shared by a number of respondents was that increasing cyber security skills more generally across the population would assist with the skills shortage. If people stopped doing 'dumb things' it would mean less work for practitioners:

> *'The solution to the skills shortage will not be solved by more security people alone but with a general elevation of cyber skills across the board and to this end It's my belief that we should be teaching better cyber skills to school children, not simply promoting STEM in schools.'*

Soft skills

The need for soft skills were highlighted by a number of survey respondents as an important consideration for cyber security workers.

> *'Highly technical resources with poor communications capability (not language skills - communications) reduce their effectiveness as much of our work is about negotiation and influence (people) not simply technical or compliance based work.'*

> *'People and soft skills are also lacking in otherwise technically qualified candidates which make them not suitable for mid-senior security roles.'*

> *'Candidates often have many certifications, but cannot effectively engage with business or other technical staff in order to complete their roles.'*

The role of consultants

In the analysis of the advertised positions, about 20% of openings were for contractors or temporary employees rather than full time employees. A representative from a large international recruitment agency confirmed that this is a relatively high number.

Around 27% of respondents indicated they currently work for consulting organisations.[17] A high number of cyber security workers employed by consultancy firms is consistent with findings by (ISC)[2] that suggest that Australia has a higher proportion of consultants than any other country in the Asia-Pacific.[18] The (ISC)[2] findings also indicate that far fewer professionals see themselves as becoming managers in Australia, while more than a third of the Australian respondents expect to be in a security consulting role in the future.

[17] This is discussed in more detail in the section headed 'Participants Details' below.

[18] In Australia, 9% of respondents were in managerial roles, while in most other countries the figures was closer to 20%. 27% of respondents in Australia were consultants, compared to around 20% across the other countries in Asia-Pacific.

One respondent commented that he had to start his own business 'as I wasn't able to gain infosec employment in Adelaide. That is despite having a Master's degree in Information Systems Security and various certifications.'

The high number of contractors and consultants in the Australian market and the expectation that information security people will move into security consulting in the future may point to a unique systemic issue in the Australian cyber security market. It may be that Australian organisations are less willing to create permanent positions for senior information security professionals or to pay the sort of salary expected by highly experienced information security specialists, instead relying on consultants for advice as required. At least one industry figure noted this growth in the use of contractors, saying that 'People are opting for a contract role because they are able to negotiate a better rate for their skills set."[19]

This prominence of contractors and consultants in the Australian cyber security landscape is of interest in the context of the cyber security skills shortage as the skills required to be a consultant are likely to be different to those required by in-house information security professionals.

The reliance on contractors and the move into consulting by advanced practitioners also may reflect a lack of maturity in the Australian cyber security skills ecosystem, with few high level, well paid in-house security roles. As one survey respondent commented:

> *I have worked in the US and Europe for over 15 years and the Chief Security Officer reports to the CFO or board. Most Australian organisations are still operating as if it's the 1990's with a CISO reporting to the CIO. This is your problem, unless that is fixed security will never be taken seriously!*

Interestingly, it may also be that consulting organisations are more willing to recruit and train entry level cyber security workers. One survey participant made the following comment:

> *Entry level positions will be available in consulting firms rather than end user organisations, as security services are outsourced more and more.*

[19]Head, B. (29 January, 2016). The need for cyber security skills in Australia balloons. ComputerWeekly.com.

Analysis of Seek.com job postings

Methodology

There were 345 cyber security job advertisements posted online via a job advertising website (www.seek.com.au) between May and July 2016. They were collected and analysed as part of this research.

The online site Seek.com.au was selected as it is one of the most popular job searching website in Australia. However, it is worth noting that many positions, particular more senior positions, are unlikely to be advertised on an online site such as seek.com.au. Accordingly, the results should not be taken to indicate a comprehensive picture of cyber security jobs available in Australian 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).

To identify relevant job postings, the following search parameters were used: 'cyber security', 'information security' and 'all of Australia' (for geographically filtering of the advertisements). In addition, jobs types that were included in the sub-category of 'Security' under the job category of 'Information & communication technology' were selected.

The advertisements were collected in four snapshots taken on 23 May 2016, 10 June 2016, 24 June 2016 and 18 July 2016 respectively. A gap of between two to three weeks between each snapshot was used in order to try to collect different advertisement samples. Where the same advertisements appeared in different snapshots, those advertisements were included in the analysis. However, where the same position appeared a number of times on the same date, it was only included once and the duplicated references were removed. We also tracked and have reported on those jobs which continued to be advertised across multiple snapshots. The continued advertising of a position may indicate difficulties in recruitment.

The software system NVivo version 11 was used to analyse the data as it supports the widest range of analysis of data sources and offers the most advanced analysis tools for qualitative and mixed methods research datasets. In the study, all the advertisements from the four snapshots were imported to NVivo as PDF files for analysis. Most of the analysis was done using the text search query option to determine trends and occurrences. However, the advertisements were also separately coded to identify the different requirements and job descriptions for advertised roles.

Within the study, job roles were selected based on the advertisements and text search analysis to determine key job types. Salary ranges were considered based on the upper and lower salary ranges as indicated via the text analysis. When analysing years of experience, certification and salary range, each advertisements was considered as a whole and occurrences and ranges were developed based upon the text analysis.

Research findings

Number and location of available positions

The availability of cyber security jobs by location is indicated in the table below. Sydney, Canberra, Melbourne and Brisbane were the locations with the highest number of job vacancies, with Sydney and Canberra showing a markedly higher number of available jobs. Very few vacancies were available in Adelaide and Perth, while there were no jobs advertised in Darwin or Hobart over the relevant periods.

Location	Date of advertisement			
	23.05.2016	10.06.2016	24.06.2016	18.07.2016
Sydney	42	38	48	48
Canberra (ACT)	27	21	15	9
Melbourne	11	15	8	19
Brisbane	11	11	4	4
Adel aide	0	2	2	0
Perth	0	3	5	2
Darwin	0	0	0	0
Hobart	0	0	0	0
Total	**91**	**90**	**82**	**82**

Figure 15: Cyber security jobs location

These findings are of particular interest given the opinion of AISA members that cyber security skills shortages were most prevalent in regional areas and in Darwin, Hobart, Perth and Adelaide. In fact, there were no advertised regional cyber security positions in the relevant period and very few advertised vacancies in Darwin, Hobart, Perth and Adelaide.

There were six cyber security vacancies posted in the first snapshot taken on 23 May 2016 which were still showing as open positions on 18 July 2016 (see the figure below). These advertisements were for analyst, architect and cyber security specialist positions in Sydney, Canberra and Melbourne. The low number of positions still being advertised might suggest that the other positions were filled or that the recruitment process may have halted for other reasons, however it is not possible to conclusively determine that this is the case without further investigation.

Job roles

The advertised cyber security jobs were categorised into job roles based on the descriptions included in the advertisements (see the figure below). The main advertised roles were analyst, consultant, manager, engineer, architect and director and CEO or owner. The 'other job' category was used to capture other types of jobs outside of those six categories.

Job Role	Date of advertisement			
	23.05.2016	10.06.2016	24.06.2016	18.07.2016
Analyst	27	16	15	17
Consultant	12	15	8	15
Manager	11	12	11	8
Engineer	9	14	11	6
Architect	6	8	10	15
Director, Owner or CEO	1	2	1	1
Other	25	23	26	20
Total	**91**	**90**	**82**	**82**

Figure 16: Cyber security job roles

The jobs most in demand were analyst, consultant, manager, engineer and architect. Of these, the cyber security analyst was in highest demand.

Experience, qualifications and certifications

Most of the cyber security jobs required prior job experience, security certifications and academic qualifications (see the figure below). Experience was specified as a prerequisite in almost all of the cyber security jobs in the data collected.

Requirement	Date of advertisement			
	23.05.2016	10.06.2016	24.06.2016	18.07.2016
Experience	88	85	77	74
Security certifications	30	30	29	25
Academic qualifications	16	12	13	5

Figure 17: Cyber security job requirements

The job roles were further sorted into sub-categories based on the wording in the advertisements and linked to the number of years' experience wherever specified in the ad. The required years of experience varied but generally each role expected at least five years' previous job experience (see below).

Job Role		No. of years
Analyst	SOC Analyst	4+
	Business Analyst	5+
	Cyber Security Analyst	5+, 5 -10
	ICT Security Analyst	2+, 3+
	Information Security Analyst	1 -4, 4+, 5+
	Intrusion Analyst	8+
	Security (SIEM) Analyst	3+, 5+
	Senior Cyber Intelligence Analyst	3+
Consultant	Cyber Security Consultant	2+ , 4+
	Lead Consultant	6+
	Information Security Consultant	3+, 5+
	Splunk Consultant	1 -3
Manager	Cyber Security Manager	3 -5, 10+
	APAC SOC Manager	Not Asked For
	Business Development Manager	5 -10
	Cyber Security Domain Architect Manager	5+
	Cyber Sec urity Programs Architecture Manager	2+
	Cyber Security Assurance Manager	Not Asked For

Engineer	Cyber Security Engineer	5+
	Information Security Engineer	Not Asked For
	Senior Security Engineer	3+, 5+, 8+
Architect	Cyber Security Architect	2 -3, 5+
	Network Security Architect	5+
	Pre -sales Cyber Security Architect	5+
	Principal Cyber Security Architect	5+
	Security Architect	3 -4, 5+
	Security Ecosystems Architect	5+
	Security Solutions Architect	2+
Director, Owner or CEO		Not Asked For

Figure 18: Required years of experience

Some advertisements did not refer to any required security certifications. However, where specified, there were often quite significant differences between the required certifications for each job role and their sub-categories (see the figure below). This is consistent with the survey findings about the lack of clarity and consistency between employers as to the skills and competencies required for similar job roles.

The most common required certification for all job roles was the CISSP. The analysis shows 95 advertisements in total asked for the CISSP certification.

Job Role		Certification
Analyst	SOC Analyst	GCIH, GREM, CCNA, CEH, OSCP, OPST, eCPTT, GSEC
	Business Analyst	Not Mentioned
	Cybe r Security Analyst	CISSP, GIAC, EC -Council, Offensive Security, CEH, GPEN, CREST, OSCP, GCIA, OLCP, GIAC - GSE, GCIH*, GREM*, CCNA, RHCE, MCSE
	ICT Security Analyst	Not Mentioned
	Information Security Analyst	CISA, CISSP, CCNP, CCSE, SANS GSEC, GCIH, GCIA
	Intrusion Analyst	SANS/GIAC (GCIH, GCIA, GMON, GREM, GCFA, GPEN, GWAPT)
	Incident Analyst	ISACA (CSX, CSXP, CSXS, CSXE), GIAC (GSEC, GCIH, GMON, GSE), EC-Council (Certified Ethical Hacker)
	Security (SIEM) Analyst	Not Mentioned
	Senior Cyber Intelli gence Analyst Cyber Security Consultant	Not Mentioned CISSP*, SANS*, GICSP, SABSA

Consultant		
	Lead Consultant	Not Mentioned
	Information Security Consultant	CISA, CISM, CISSP, GIAC, GCFA, SABSA
	Splunk Consultant	Not Mentioned
Manager	Cyber Se curity Manager	OPST, OPSA, GSEC, CEH
	APAC SOC Manager	CISSP, CISM
	Business Development Manager	Not Mentioned
	Cyber Security Domain Architect Manager	Not Mentioned
	Cyber Security Programs Architecture Manager	Not Mentioned
	Cyber Security Assurance Manager	CISA*, CISM*, OSCP, CEH, SAN
Engineer	Cyber Security Engineer	Not Mentioned
	Information Security Engineer	CISSP
	Senior Security Engineer	CISSP, CEH, CISA, CISM, IISP
Architect	Cyber Security Architect	CISSP, CISM
	Network Security Architect	CCIE
	Pre -sales Cyber Security Architect	CISSP
	Principal Cyber Security Architect	SABSA, CISSP, CISM, SANS, TOGAF, CEH, CESG, ISSP
	Security Architect	CISSP, CompTIA Security+, CCNA Security, GIAC, MSCE, IRAP, CISM, CISA
	Security Ecosystems Architect	CISSP*, SABSA*, CISM, CPTE, CEH, GIAC
	Security Solutions Architect	CISSP, CISM, CEH, ITIL
Director, Owner or CEO		Not Mentioned

* Denotes highly considered certification

Figure 19: Required certification

Most of the jobs in Canberra required a security clearance, as the majority of these jobs were advertised by government organisations (see the figure below). A few jobs in Sydney and Melbourne also required security clearances.

Location	Date of advertisement			
	23.05.2016	10.06.2016	24.06.2016	18.07.2016
Canberra (ACT)	12	19	12	8
Sydney	0	2	1	3
Melbourne	0	0	0	1

Figure 20: Security clearance as a requirement

Salaries

Most of the advertisements did not include any particular specified salary for the job role, noting that the salary was negotiable (see the figure below). Details of the salary ranges for those jobs where it was specified are included in the preceding Section in the consideration of salaries offered in different locations.

Salary	Date of advertisement			
	23.05.2016	10.06.2016	24.06.2016	18.07.2016
Mentioned	25	20	24	24
Not mentioned	66	70	58	58
Total	**91**	**90**	**82**	**82**

Figure 21: Availability of salary information in advertisement

Participants' Details

Over 400 AISA members completed some part of the survey. Over 350 participants completed the entire survey. As part of the survey, a series of questions were asked to provide more detail on the AISA member community. Based on those responses the survey participant cohort can be described as follows:

Gender

Over 87% were male, around 10% were female and the balance preferred not to specify a gender.

Age and experience

Participants were asked to indicate which age bracket they belonged to. More than 75% of responses were provided by people aged over 36, with 42% aged between 36 and 45, 22% between 46 and 55 and 11% aged over 55.

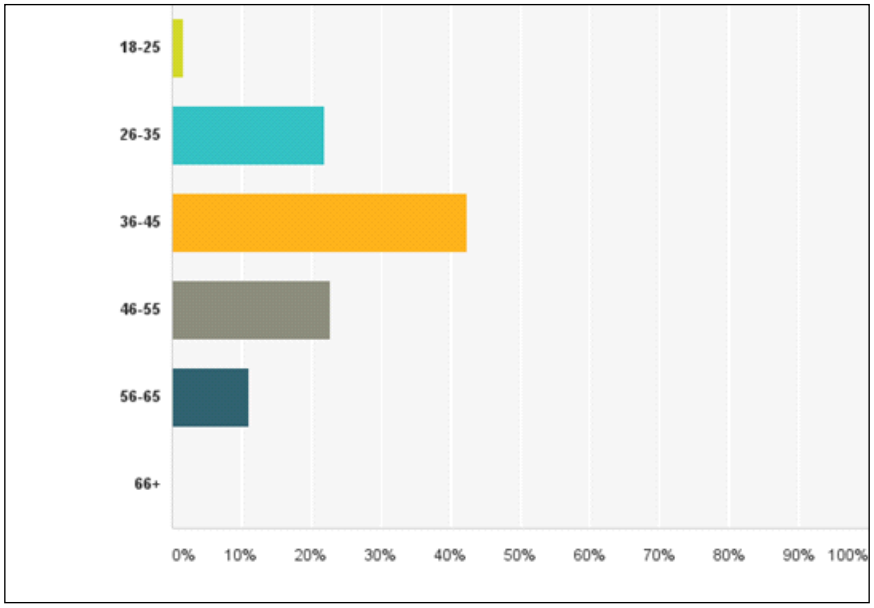


Figure 24: Age of participants

Consistent with this picture of a middle aged profession, over 48% of the AISA members who responded had at least 10 years of cyber security work experience.

Years of experience	% of respondents
Less tha n 3 years	15%
3 – 5 years	14%
6 – 10 years	23%
11 – 20 years	35%
More than 20 years	13%

Figure 25: Years of cyber security work experience

A number of respondents referred to the problem of the aging cyber security workforce, noting it as a particular concern:

> *My understanding is that the average age of cybersecurity professionals is 40+ which means that there are a lot of us ready to retire. This will have a serious impact on the ability of organisations to resource security properly.*

Education and certifications

The section of the Australian cyber security profession responding to this survey are highly educated. More than 70% hold a bachelor degree or higher.

Answer Choices	Responses
Less than High School	0.73%
High School or equivalent	8.05%
TAFE Certificate or Diploma	13.66%
Associate Degree	3.66%
Bachelor's Degree (BA, BSc etc)	39.27%
Master's or Doctoral Degree (e.g. MA, MS, MEng, MEd, MSW, MBA, PhD)	30.49%
Other (please specify)	4.15%
Total	

Figure 26: What is your highest level of education?

The CISSP was the most widely held certification, followed by the CISM and CISA. Many respondents also held different GIAC Certifications and others indicated that these were the certifications that they would be pursuing. Other certifications that many practitioners held included PRINCE2 and ITIL.

Areas of expertise and job roles

Although AISA is often regarded as being a technically focused organisation, the majority of survey participants indicated that their position was one of management rather than a more technical role. Thirty-one per cent of respondents indicated their area of expertise was business management, versus 19% who regarded themselves as involved in managing technical issues.

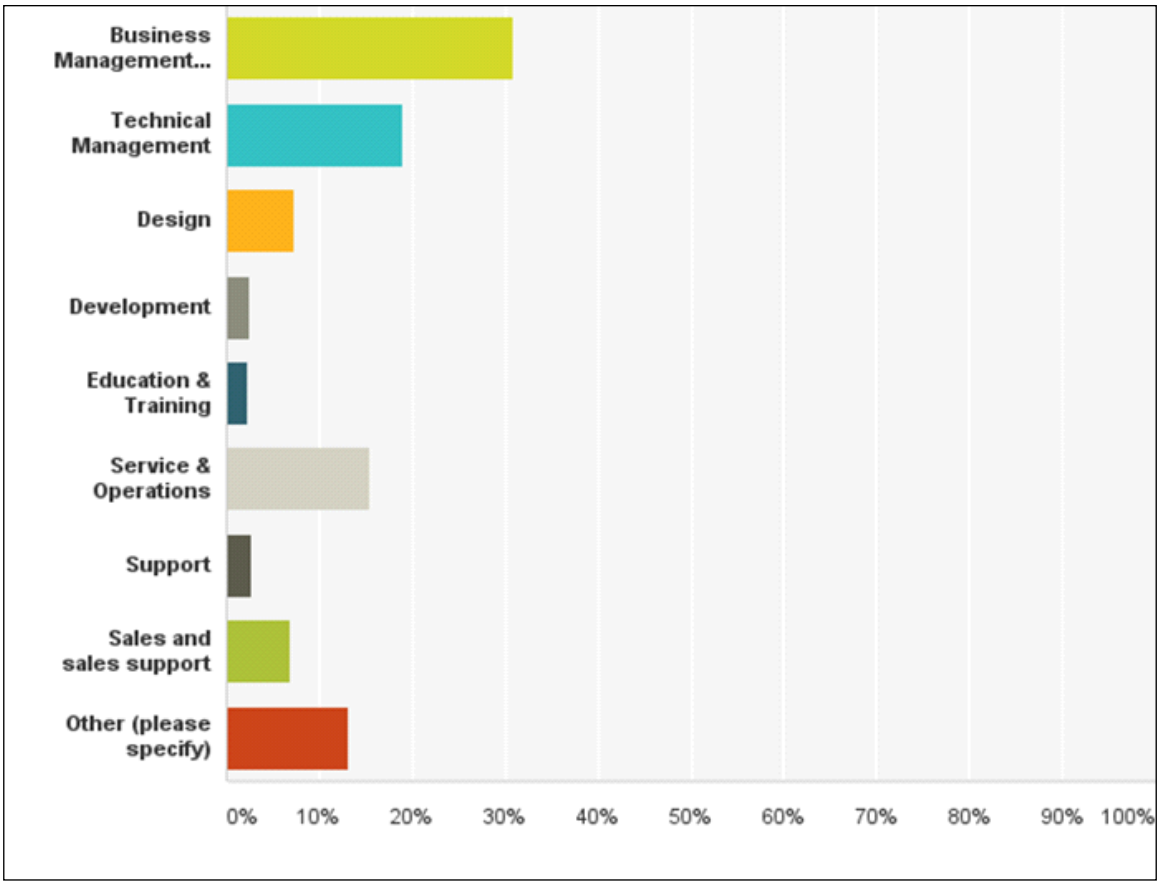


Figure 27: General area of information security expertise

Areas of expertise indicated by those selecting 'Other' include research and tester.

Most cyber security workers were full time employees. Ten per cent of respondents indicated they were either self-employed or the owner/director of a business. Less than 1% of employees held part-time positions.

Respondents were asked to indicate the job titles closest to the one they held, with different titles provided for those respondents who worked for end-user organisations and those who worked for other organisations, including vendors, consulting firms and professional services organisations.

For end user organisations, the main job roles were Security Managers, Security Administrators and Architects. There were very few trainers, awareness specialists or privacy officers. There were also no respondents who indicated they were part of procurement or logistics, which is of interest given the increased usage of outsourced and cloud based services, including security services.

Job Titles: End User Organisations		
Job Title	**No. with this title**	**% of total**
Security Manager or IT Security Manager	32	19%
Security Administrator, adviser or analyst	25	15%
Architect	19	11%
IT Manager	11	7%
Governance, Risk and Compliance Manager including Risk Manager	11	7%
C-level Security Manager	10	6%
Security Operations	9	5%
Incident Handler or investigator	7	4%
Auditor, certif ier or assurance manager	5	3%
Security Engineer	5	3%
Security Consultant & Security advisers	5	3%
Researcher & university lecturers	4	2%
Project Manager	3	2%
Security awareness practitioner	3	2%
Developer	3	2%
Director, Owner, CEO	3	2%
Business analyst	2	1%
Network Administrator	2	1%
Other	8	5%
Total	**167**	**100%**

Figure 28: Job Titles – End User Organisations

Looking at consulting organisations, vendors and professional services organisations, 35% of respondents were consultants, while another 10% were account managers and 10% were architects. Again, there were few respondents who identified as security awareness specialists, trainers or privacy professionals or as being part of procurement.

Job Titles : Consulting Organisations, Vendors and Professional Services Organisations		
Job Title	**No. with this title**	**% of total**
Consultant - security management including ISO 27001, ISM	47	20%
Account manager, Sales Manager, Channel Manager	24	10%
Architect	24	10%
Consultant - technical	35	15%
Owner, Director, CEO	30	12%
Security Analyst, business analyst	17	7%
Sales Administrator, pre-sales support	5	2%
Operations Manager, Security Operations Manager	5	2%
Auditor, certifier or accreditor including PCI DSS QSA, iRAP	8	3%
CISO, Head of Security, Security Director, CTO	6	2%
Tester - vulnerability testing, penetration testing, application testing	6	2%
Forensic expert	4	2%
Incident investigator	4	2%
Product Manager	4	2%
Information Security Manager, Information Security Officer	5	2%
Engineer	4	2%
Privacy or data protection specialist	2	1%
Developers and programmers	2	1%
Other	9	4%
Total	**241**	**100%**

Figure 29: Job Titles – Consulting Firms, Vendors, Professional Service Providers

A high number of respondents identified themselves as owners, directors or CEOs.

This is consistent with the high number of smaller consulting organisations in Australia. Respondents were asked to indicate the size of the organisations that they worked for. At least 57 members responded that they worked for consulting firms or professional services organisations with between 0 – 19 staff. Seventy-five of respondents worked for organisations with 500+ staff.

Employers and Industry Sectors

Over 65% of respondents worked for large organisations that is organisations with 500 or more employees, with close to 55% working for organisations with 1500 or more employees. Conversely, approximately 20% worked for organisations with 19 or less employees.

Less than half of the respondents (42%) worked for an end user organisation. The balance was divided between security consultancy organisations, vendors and professional services organisations such as law firms.

Answer Choices	Responses
End user organisation	42.16%
Vendor	16.91%
Consultancy firm	26.96%
Professional services organisation e.g. law firm	13.97%
Total	

Figure 30: Description of the organisation you work for

Of those respondents who worked for end user organisations, the main employers were in the following industry sectors:

Industry Sector	Responses
Financial/Banking/Insurance/Financial Services	22%
Federal Government including the ACSC	15%
State Government	12%
Education/Training	11%
Utilities	7%
Retail/wholesale/distribution	5%
Telecommunications/communications	5%
Healthcare/Medical/Health Services	4%
Local Government	3%
Other	7%

Figure 31: Industry sector of employer organisations

Aggregating the numbers, approximately 30% of respondents work for Federal, State and Local Government; 22% are in the financial sector and more than 11% in education. This is consistent with data provided in terms of the size of the employer organisations. Fifty-five per cent of respondents worked for organisations with more than 500 employees.

Geographical Location

AISA was interested in where its members are currently working. Participants were asked to provide the postcode for their work address. The figure below shows where the participants in this survey currently work.

Workplace Location	Responses
Sydney	105
Melbourne	93
Brisbane	64
Perth	53
Canberra	33
Adelaide	25
Regional NSW	9
Regional VIC	1
Regional QLD	4
Regional WA	1

Figure 32: Location of workplace

It is of interest that few AISA members are located outside major capital cities. This may bereflective of AISA's presence (or lack thereof) in those areas. AISA has recently established branches in Darwin and Hobart and is keen to serve regional Australia.

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 3000 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.

Our independent non-profit association 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.

For more information about this report please contact:

Mr Arno Brok

CEO, AISA

Arno.brok@aisa.org.au

Dr Jodie Siganto

Director, AISA Cyber Security Academy

Jodie.siganto@aisa.org.au


AISA

ABN 181 719 35 959
Level 8, 65 York Street, Sydney NSW 2000