CYBERSECURITY TALENT STUDY

A deep dive into Australia’s cybersecurity skills gap
The global shortfall in cybersecurity skills has been well-documented, with studies repeatedly confirming most companies are struggling to find, train, and keep suitably skilled cybersecurity staff.

While the existence of the skills gap itself is clear, many cybersecurity staff struggle to name the skills they think their organisation needs – or the skills that would help progress their own cybersecurity careers.

A lack of definition around required skills suggests that it is not just the skills themselves that are missing, but the talented individuals necessary to provide and integrate those skills into the everyday operations of the business.

To this end, McAfee’s Cybersecurity Talent Study set out to identify the deficiencies in cybersecurity talent that companies face today, and to better understand the dynamics that are preventing existing cybersecurity specialists from delivering the capabilities businesses need.

The online study, conducted by independent research consultancy StollzNow Research, was completed in August 2018. The study included 216 respondents drawn from a panel of Australians working in the cybersecurity industry, including 150 from within organisations with 250 or more staff, 53 McAfee customers, and 13 McAfee staff.

Analysis of the results revealed some interesting trends:

- Most cybersecurity staff believe they already embody the characteristics that their colleagues should aim for as well.
- Women are participating in Australia’s cybersecurity workforce at much higher rates than the global average.
- Cybersecurity experts follow a range of career paths to get into their current positions.
- Strong associations between cybersecurity skills and gaming suggests companies should factor gaming habits into cybersecurity hiring.

These and other findings paint a portrait of a multifaceted workforce that has aligned itself around a number of core attributes – but still lacks a coherent vision of the characteristics necessary to expand and diversify Australia’s talent pool.

By leveraging these findings to refine staff development and recruitment strategies, companies may find the answer to relieving cybersecurity staffing pressure lies not in hiring more of the same kinds of people, but in recognising the many drivers that steer employees into cybersecurity careers – and using those drivers to capture an even broader array of talent for the future.
Key Findings

- Australia’s cybersecurity workforce is 25% female, according to the survey. This makes Australia more than twice as high as its global counterparts when it comes to female employees in cybersecurity, with global research showing just 11% of cybersecurity workers are female. Although Australia is making a step in the right direction, there is still work to be done to achieve gender equity goals.

- Respondents had similar ideas of the qualities that made them good cybersecurity workers, and which qualities were desirable in other people. These included: the ability to translate technical concepts into plain language, analytical capabilities, working well in a team, and good communications skills. However, 27% of respondents couldn’t identify a single skill that made for a good cybersecurity worker. These findings suggested there is still a lack of consensus about the skill set required for an effective cybersecurity employee, as well as a lack of understanding of what a truly diverse team should look like – which threatens efforts to build well-rounded, effective organisational cybersecurity capabilities.

- Most cybersecurity workers (84%) have tertiary degrees – with 49% of those in engineering, information technology (IT), telecommunications and cybersecurity – while 49% have no cybersecurity certifications at all. Just 16% said they have worked in another industry or a non-IT role. Recruiting cybersecurity workers just from the IT industry is unlikely to bolster diversity and can limit new thinking – a potentially dangerous shortcoming in an industry as dynamic and fast-changing as cybersecurity.

- Most cybersecurity staff are working in operations or management rather than in strategy, education, or advisory roles. Only 34% of respondents said they spend over half their time working in cybersecurity. At the same time, 57% of managers said they have trouble finding staff – and operations staff are the hardest to come by, cited as ‘difficult to source’ by 62% of respondents. These figures suggest many staff are still juggling cybersecurity responsibilities with other job functions, limiting their ability to dedicate their time to cybersecurity, and constraining the company’s responsiveness. Such figures reinforce the case for automation, which would allow cybersecurity workers to spend more time on strategic and holistic tasks, rather than tactical and reactive work.

- Strong correlations between gaming and cybersecurity work suggest gamers represent a significant potential source of cybersecurity workers. Most cybersecurity workers polled (69%) said they either are, or used to be, keen gamers. This finding, which reflects previous McAfee research, suggests managers may want to consider gamers as forerunners when looking for cybersecurity staff.
The state of play for cybersecurity talent

Like every country, Australia is facing a crisis in cybersecurity staffing. An expanding attack profile is increasing pressure on existing cybersecurity staff. Yet the pipeline of available talent has thinned considerably due to overwhelming demand and fierce competition for a small base of skilled employees.

Australia’s Cyber Security Strategy, published in 2016 by the Department of the Prime Minister and Cabinet (DPMC), highlighted some of the challenges facing the industry. Demand for cybersecurity services and related jobs will grow by at least 21 percent through 2021, the report notes, while take-up of ICT-related university degrees has halved over the last decade.

The workforce is also struggling with gender diversity: the strategy notes Australia’s workforce ‘suffers from low participation from women,’ who (ISC)² and Frost & Sullivan note comprise just 11 percent of information-security professionals worldwide. This ‘means we are not harnessing the full potential of our talent pool,’ the DPMC report notes.

Equally challenging is ensuring Australian industry has access to the range of expertise necessary to build a diverse workforce. This cybersecurity workforce must possess management skills, strategic thinking, and operational cybersecurity skills. These are necessary to address cybersecurity’s critical role as an enabler of corporate governance, legislative compliance, risk minimisation, and to support strategic business initiatives.

McAfee’s Cybersecurity Talent Study sought to identify key attributes and deficiencies within Australia’s cybersecurity workforce, with the aim of identifying core strengths and areas where the country’s talent base would benefit from further development.

The study’s results confirmed Australian businesses are struggling to get enough talented cybersecurity specialists, with 57 percent having trouble finding cybersecurity staff.

Indeed, 62 percent of respondents said that security operations staff were hard roles to fill, while 55 percent said strategy-related roles were hard to fill. Other roles which were identified as difficult to fill included administration and IT operations (27 percent) and audit, compliance, and regulation (23 per cent).

As well as confirming the talent gap remains a salient issue, the research also identified some surprising characteristics of Australia’s cybersecurity workforce – including a higher-than-average proportion of women, and a disconnect between individuals’ perceptions and expectations of their own abilities, versus those of their colleagues.
Australia ahead of the curve in gender equality

The globally benchmarked Global Information Security Workforce Study suggested that women comprise just 11 percent of cybersecurity workers globally.

Just one percent of the C-level executive global cybersecurity workforce was female, with a further five percent comprised of female directors, managers, or middle managers. Six percent were female non-managerial staff or entry-level.

The results of McAfee’s Cybersecurity Talent Report, however, painted a very different picture of the gender split within the Australian cybersecurity workforce. 25 percent of respondents were women – more than double the global average.

This aligns more closely with figures such as the Australian Cyber Security Centre’s recent report that half of its leadership group, and 30 percent of staff in its Cyber and Information Security Division, are female.

The figures are encouraging indicators for female participation in the local cybersecurity industry. While this is a step in the right direction, there is still work to be done to achieve gender equity goals.

“Women comprise just 11 percent of cybersecurity workers globally...but 25 percent of the Australia-focused Cybersecurity Talent Report respondents were women, suggesting that efforts to engage Australian women in cybersecurity careers are being implemented with consistent success.”
Many paths to cybersecurity

To date, many efforts to bolster cybersecurity qualifications have focused on supporting tertiary and postgraduate courses, either with subspecialties in cybersecurity or by incorporating cybersecurity into broader courses teaching ICT (information and communication technology) skills.

Many respondents to the *Cybersecurity Talent Study* reflected this focus, with 84 percent of respondents indicating they had undergone formal education, and 49 percent of under 30-year-olds saying that they had been in the industry for five years or less.

This result suggested that cybersecurity is succeeding in attracting new workers, with many seeing it as an attractive career pathway upon leaving school or university.

However, 49 percent said their formal qualifications were in engineering, IT, telecommunications, or cybersecurity – reflecting an ongoing bias towards technically-trained employees in cybersecurity roles. Far fewer respondents came from business, finance, arts, science, and other areas of study – highlighting the challenge the cybersecurity industry continues to face in attracting people with established careers, who are looking for a new challenge, as well as new graduates in these disciplines.

It also shows the industry needs to do a better job of attracting people with varied ideals, thinking, and views that can be gleaned from a wider range of education.
Respondents reported past experience in a broad spectrum of professions and trades including sales, accounting, marketing, teaching, food services, sports management, civil engineering, and retail. People with non-technical skills have much to offer cybersecurity, and people with established problem-solving skills often find great intellectual challenge in applying them to cybersecurity issues.

While university-level training is arguably important in producing cybersecurity leaders and thinkers, recognition that universities alone cannot satisfy demand for cybersecurity workers has driven the industry to think outside of the traditional box.

Along similar lines, the Victorian State Government, for its part, recently moved to make the TAFE-level Certificate IV in Cyber Security available to anybody for free. And Telstra Business Technology Services (BTS), for one, has targeted both technical and non-technical staff with a BTS Academy program that shepherds staff through an intensive training and mentorship program. One recent cohort saw around two dozen staff achieve 101 technical qualifications, as well as professional recognition by the Australian Computer Society.

The notion of a skills shortage is notable due to the bridge between the shortage itself and what skills are actually missing. 78 percent of survey respondents believe there is a skills shortage in cybersecurity, but 63 percent of this group don’t know what skills are missing.

This begs important questions about how these companies are hiring, and how management is briefing human resources teams to fill these roles – including filtering by qualification and experience.

Company size and resources seem to be a factor. Qualifications are much less common in small businesses (<250 employees), in which 54 percent of respondents said they had no cybersecurity qualifications. This was well behind the 24 percent of respondents from mid-sized companies (250 to 500 employees) who said they had no such qualifications – exposing a stark contrast in the companies’ relative investments in skills training.

“Two-thirds of surveyed staff (i.e. non-managerial) in the study said they had no cybersecurity certifications – suggesting that many companies are hiring cybersecurity staff without investing the time and money to develop those employees’ skills to meet specific areas of demand.”
The impact of underinvesting

Respondents said that many employers treat cybersecurity as a single job description – something that one respondent said had led to ‘ridiculous’ job advertisements in which companies ‘are looking for multi-skilled people [capable of managing] desktop security, firewalls, application security, security analytics, and more – all in one person.’

Each of these operational areas requires a different, specialised skill set, but there were signs that cybersecurity staff are being treated as generalists rather than specialists.

On average, for example, both small businesses and medium-sized businesses had 9.7 cybersecurity employees. This suggests managers in medium-sized businesses expect cybersecurity employees to do much more work than those in small business. Looking after up to 500 employees, after all, is much more demanding for a cybersecurity team the same size as those in companies with fewer than 250 employees.

This strategy also implies that the cybersecurity staff in medium-sized businesses are expected to multi-task more and be able to manage a broader range of cybersecurity activities. Even larger companies, with more than 500 employees, were also expecting a lot from their cybersecurity workers, with teams of just 11.4 people on average.

Mid-sized companies reported much less trouble finding security operations staff, with just 38 percent reporting problems compared to 75 percent of respondents from small and large companies.

Measures of hours worked also varied dramatically, with 84 percent of cybersecurity workers in small businesses working 31 to 50 hours per week – but just 62 percent of mid-sized company employees working as much. In fact, the study shows 32 percent of mid-sized company employees worked 30 hours or fewer per week.

These anomalies suggest mid-sized companies may have more part-time employees, perhaps because they are pushing towards a cybersecurity model that is built more around sourcing specialised skills from different people.

It may also reflect the tendency for mid-sized companies to outsource their security operations. This can be a direct impact of the cybersecurity skills shortage, but also because mid-sized companies are often expanding their operations and need a service partner that can provide consistent service levels across the business.

It may also be because mid-sized organisations are more effective in luring new staff straight out of university. Whereas 79 percent of respondents from smaller companies were transitioned into cybersecurity roles from other ICT positions, mid-sized companies are recruiting heavily from universities – with 46 percent of respondents.
saying they began working in cybersecurity immediately after finishing their education.

This suggests that small companies are either struggling to offer competitive employment packages for recent graduates, or simply can’t offer the perceived career prospects that a larger organisation can provide.

Respondents from mid-sized companies also showed significant aberration in terms of the attributes that they possess. In nearly every measure, significantly fewer respondents from mid-sized companies said they possessed most of the skills involved in being a good cybersecurity employee.

This may reflect a culture of outsourcing, implying cybersecurity skills and traits had been pushed outside the organisation – or that the existence of such strategies had left internal staff feeling less than capable when it comes to cybersecurity. It may also reflect the presence of more recent university hires, who may not yet be as confident in their abilities.

“Some respondents pinned the shortcomings on their managers’ commitment to cybersecurity development, with one noting, ‘cybersecurity has been an after-thought by managers in this geography for a long time. IT management... have been accountants and not IT-aware for too many years.'
What makes a good cybersecurity worker?

This lack of investment in training may well be due to a lack of resources and time, but McAfee’s *Cybersecurity Talent Study* findings suggest other issues may also be holding back such investments.

Specifically, the results suggested there is considerable confusion about just what skills and traits are necessary to be considered a good cybersecurity worker.

The most common answer, named by just 20 percent of respondents, was having good skills and product knowledge. Respondents also said cybersecurity staff should be analytical (named by 12 percent), creative (10 percent), meticulous (10 percent), diligent and focused (nine percent), and have an appetite to learn (nine percent).

Challenges around self-perception, especially when filling cybersecurity skills, have implications for cybersecurity managers charged with building and executing effective operational teams. Gaps in particular skills may be cause for them to invest in targeted staff training – or automation tools that can take over much of the low-value, operational processes involved in cybersecurity work.

Identifying those gaps, however, can be complicated: 73 percent of respondents believe they could do their job better, but 49 percent were unable to say what specific cybersecurity skills they needed.
Most believe other cybersecurity employees should have similar attributes to those that they themselves possessed – including the ability to translate technical concepts into plain language, analytical skills, working well in a team, and good communication skills with others.

Yet, this suggests many cybersecurity employees don’t appreciate the need for a diverse team, which would involve hiring staff with different attributes, study backgrounds, and personality traits to complement their team’s deficiencies.

“Identifying deficiencies proved also tricky. A similar proportion of respondents (47 percent) said they couldn’t name what cybersecurity skills their organisation was lacking, with the largest single answer – cybersecurity fundamentals – named by just 16 percent of respondents.”

This concerning answer suggests many cybersecurity employees are struggling to keep up with the basic concepts that underpin their everyday work – which can, in turn, negatively impact team performance and compromise the effectiveness of the organisation’s cybersecurity defences.

Efforts to resolve this issue may benefit from work such as the Skills Framework for the Information Age (SFIA), which correlates a range of ICT jobs against more than 100 different skills and attributes. Employees can use these characteristics to match their capabilities against their current or desired roles, while employers can use them to better plan the training and hiring practices they should be aiming to develop.
Mixed expectations affecting collaboration

Personality traits introduce other complexities in team building. When asked what attributes they feel they possess, respondents overwhelmingly named their ability to translate technical concepts to plain language for those outside of IT, their analytical skills, their ability to work well in a team, and their good communication skills with co-workers.

Also important were the ability to work well under pressure, their ability to be task-focused, and their ability to think outside of the box.

Interestingly, respondents expected more of their colleagues in a number of areas. For example, while 38 percent said they are proactive rather than reactive, 46 percent expected their colleagues to be this way. And while some 44 percent said they work well under pressure, 50 percent expected their peers to do so.

These figures suggest many cybersecurity professionals are looking to their colleagues to work harder, perform better, and be more effective.

Conversely, several responses suggested cybersecurity employees were more confident in their abilities than those of their colleagues: for example, 51 percent said they work well in a team, but only 41 percent expected their colleagues to be able to work well in a team.

37 percent said they were able to translate technical concepts into plain language, while just 27 percent said it was important for their peers to be able to do the same.

And while 38 percent believe they have good presentation skills, just 24 percent said these attributes are important in other workers.

These figures suggest that many cybersecurity employees see their role as educators and subject-matter experts, rather than people who are eager to learn from their colleagues. This reflects a challenging dynamic for managers, whose core job responsibilities include fostering a collaborative spirit amongst the people they are directing.
The new rules of the game

McAfee’s *Cybersecurity Talent Report* identified that 44 percent of respondents were keen gamers. Gaming was heavily linked to age, with two-thirds (67 percent) of cybersecurity staff younger than 30 saying they are keen gamers, and a similar proportion of those over 50 (63 percent) saying they had never been a gamer.

Company size also showed a strong link to gaming habits. Just seven percent of small business respondents, for example, said they were keen gamers while 51 percent of those in mid-sized businesses and 48 percent in large businesses said the same.

Similarly, 68 percent of small business respondents said they had never been a gamer – more than twice the proportion of companies in mid-sized (25 percent) and large (26 percent) companies.

These figures suggest either small businesses are not thinking laterally enough in selecting their cybersecurity staff, or they are failing to offer the breadth and depth of problem-solving challenges that would attract gamers to roles within their company.

Either way, small businesses may be particularly well advised to explore ways to tap into Australia’s large base of game-playing potential employees: the recent *Digital Australia Report 2018*, for example, noted 67 percent of Australians play video games, 77 percent of players are adults, and 46 percent are female.

---

“Many of the attributes that make good gamers – problem solving, competitiveness, love of an intellectual challenge – also help cybersecurity engineers adapt their strategies for protecting networks and dealing with potential threats or business interruption.”

---

These results have been reinforced in previously documented studies such as McAfee’s *Winning the Game*, in which 92 percent of cybersecurity managers said gamers have skills that make them suited to a cybersecurity career. A further 75 percent of cybersecurity managers said they would consider hiring a gamer even if they had no cybersecurity training or experience.
Interestingly, the *Cybersecurity Talent Report* suggested that even young cybersecurity staff had already honed their problem solving and other skills from an early age: 42 percent of those younger than 30 said they had been working in cybersecurity for five to 20 years.

For such young employees to have so many years of experience suggests many came into cybersecurity as an intellectual challenge during their teenage years. Whether their career progression was shaped by employers or just by their own curiosity is not clear.

What is clear, however, is that those employees have arrived in the market with a range of relevant skills and a burning interest in cybersecurity. If employers want to take advantage of that talent, it is incumbent upon them to find ways to harness those skills, and to develop them in ways that position the company for success in the future.
To discuss the state of cybersecurity talent in Australia, or to access the full survey results, contact us via:

anz_marketing@mcafee.com
or +61 2 9761 4200