Talent

Cyber Security

Market Snapshot

About Talent

Talent is a global leader in tech and digital recruitment. From Brisbane to Berlin, we are passionate about connecting cyber security specialists with our clients around the world.

With a presence across 16 cities, we have an insatiable drive to do things better - from supporting the start-up scene via our Talent Unleashed programme, to reshaping the contractor experience with Talent Engage, and supporting young people with challenging barriers to employment through our foundation Talent RISE.

2018 WINNER:

// SEEK Large Recruitment Agency of the Year - Australia

// SEEK Medium Recruitment Agency of the Year - New Zealand

// LinkedIn Most Socially Engaged Staffing Agency Australia

// APSCo Corporate Social Responsibility Award

// Gold Medal HRD Employer of Choice Award (Medium Employers Category)

Australia's market

As we head into 2019, we are continuing to experience strong demand for technology and digital skills and a shortage of suitably skilled candidates.

With continued investment in technology-related projects and transformation programs, we are likely to see an increase in contract rates and permanent salaries at a rate above inflation.

And what about Cyber Security you ask? Business environments are constantly changing thanks to globalisation and technological advancements – but with this interconnectedness comes the risk of cyber-threats. That's where you come in!

Where are we seeing growth?

Information Security: do the words "data breach" strike fear into your very soul? Yes? Well it's not just you – organizations Australia wide are putting a lot of time and attention into securing their data.

Cyber-Security Awareness: it's important to build a human firewall and educate everyone in an organization about the importance of security. There's been a real focus on building cyber awareness in employees recently – no more money being sent to Nigerian princes!

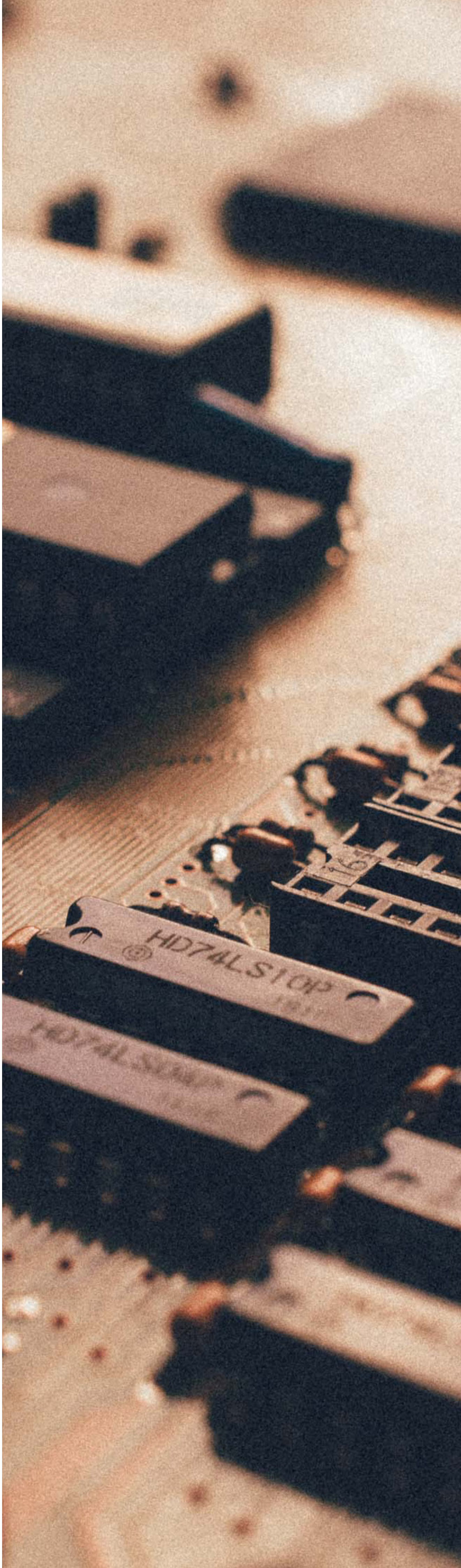
GRC: cyber security affects everyone; employees, managers, customers alike. Nobody wants their personal information accessed by people it wasn't meant for – and with the average breach costing Australian businesses $3.86million we're seeing companies ramp up their governance, risk and compliance initiatives to instil best practice!

Salary guide

We know the market here in Australia is busy and thriving – so what should you be being paid?

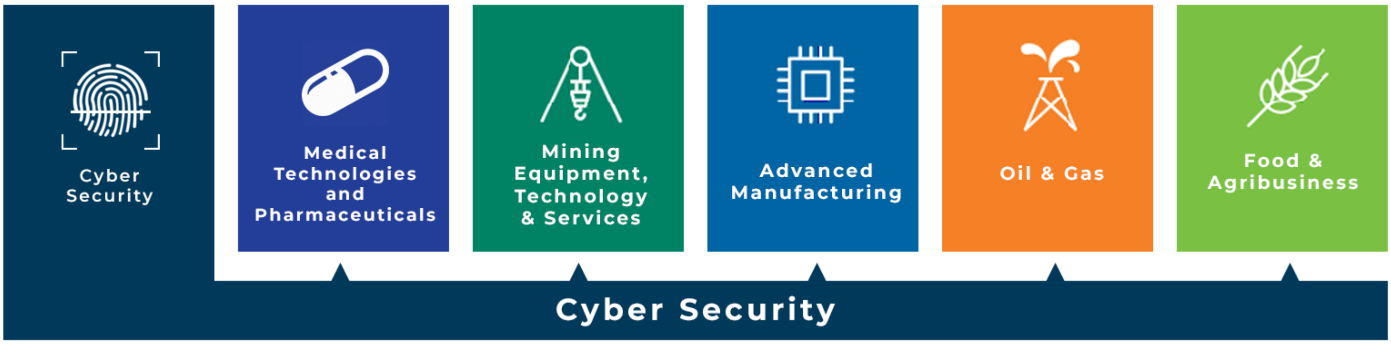
Cyber Security	
Security Analyst	$90K - $130K +
Senior Security Analyst	$130K - $150K +
Security Engineer	$80K - $140K +
Security Architect	$110K - $180K +
Cyber Security Project Manager	$120K - $200K +
CISO	$140K - $210K +

*Salaries are exclusive of superannuation



The Australian Cyber Security Market

Cyber security in Australia is a small but fast-growing sector according to AustCyber. Across Australia an estimated 19,500 people are employed and total expenditure sits close to A$4.6billion. These numbers are only set to grow, in fact the forecast suggests that revenue will triple over the next decade; Australia has the ability to take advantage of this growth opportunity to become a world leader in this field.



Cyber Security

Medical Technologies and Pharmaceuticals

Mining Equipment, Technology & Services

Advanced Manufacturing

Oil & Gas

Food & Agribusiness

Cyber Security

AustCyber's proposed roadmap focuses on the potential that cyber security has as a horizontal sector to enable growth in Australian priority sectors (as above). Three key themes were identified that together can improve Australia's cyber security posture to fully take advantage of the market shift towards digital. These themes were:

Trusted Ecosystem

– creating digital ecosystems that are highly trustworthy, promote rapid exchange of information and lead to a stronger environment for trade.

Secure by Design

– focused on ensuring new products, services, platforms and processes are designed with cyber security as a key consideration. This includes embedding more cyber security aspects into information technology courses, establishing a baseline for built in cyber security in products, and research/industry collaboration.

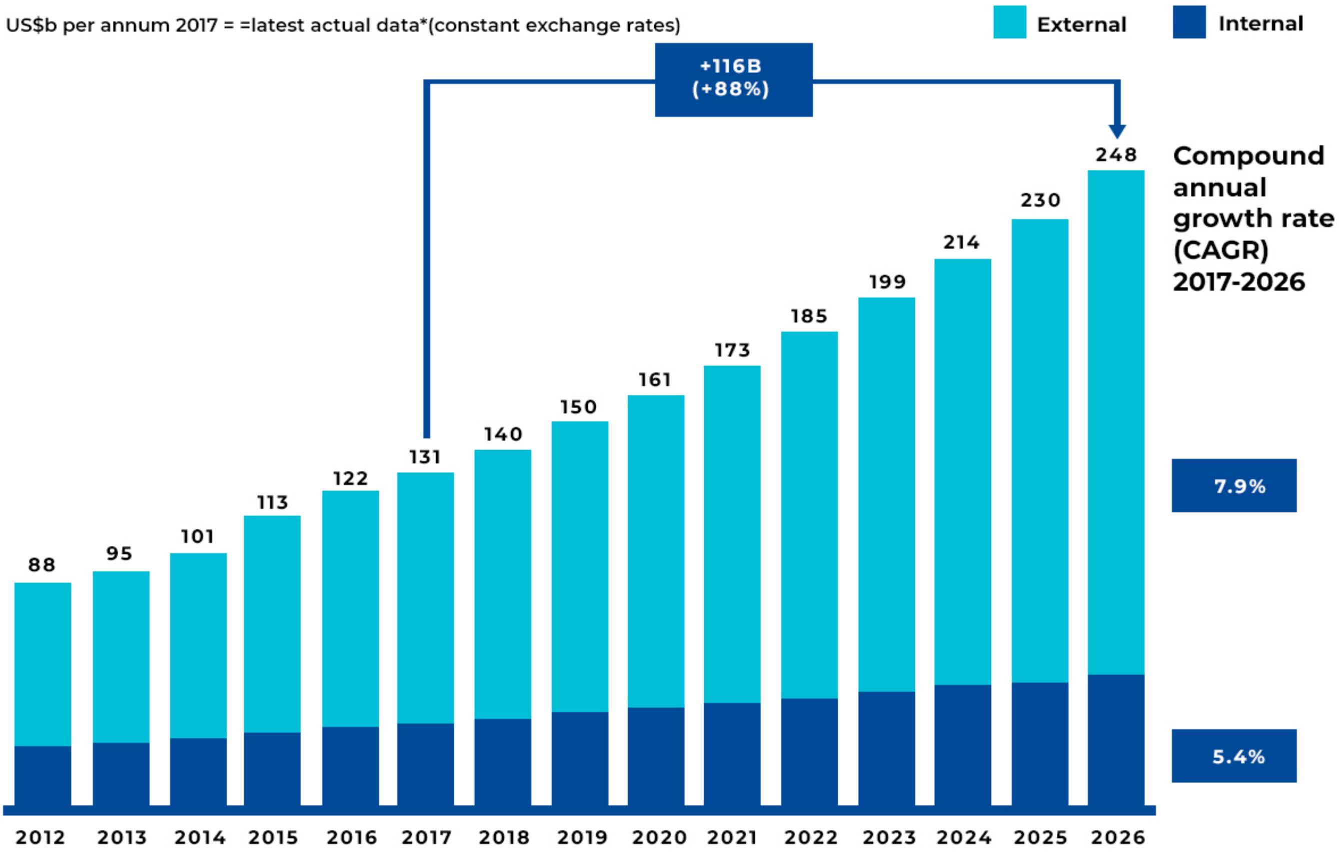
Robust and Resilient

– building greater cyber maturity and resilience in Australian industries and communities by developing a robust security culture. This involves a focus on promoting strong cyber security literacy in leadership, implementing new frameworks and improved governance to enable innovation while prioritizing resilience, and making the workforce aware of cybersecurity basics.

Cyber Security Demand

AustCyber released an update to its Cyber Security Sector Competitiveness Plan late last year which detailed the rapid growth and evolution in the security sector across both Australia and the globe. According to research, the global security market is currently worth approx. US$131 billion and is set to increase by a whopping 88% by 2026 – bringing it to US$248billion.

Figure 2 - Global cyber security spend



- 2012-2016 data based on Gartner data as at 3Q16; 2017 and beyond based on Gartner data as at 4Q17
- External spend based on forecasts to 2020 provided by Gartner extrapolated to 2026 using the average growth rates from 2017-2021. Growth rates applied at the product segment level.

§ Internal spend refers to the compensation of in-house full-time equivalent employees estimated based on Gartner data on global internal spending. Internal spend grows more slowly than external spend, linked to the increasing adoption of external managed security services

SOURCE: Gartner: Australian Bureau of Statistics: Burning Glass; expert interviews: AlphaBeta and McKinsey analysis

AustCyber has identified several trends that are driving this high level of demand across the industry;

Expanding threat of cyber attacks

There has been many examples of malicious cyber activity over the past decade and seemingly an increase recently. Symantec Corporation discovered more than 430 million unique pieces of malware in 2015 (36% increase from 2014), malicious emails cost Australia businesses more than A$20million in 2016/17 (up 230% to the year prior) and IBM reported an increase of 64% in reported security incidents from their average clients.

Mounting exposure to cyber risk

Internet enablement and the interconnectedness of devices/ systems increase the likelihood of widespread malicious cyber activity. As more people come online and everyday items like phones, watches, fridges and cars are connected to the internet more information is shared electronically which increases risk and gives perpetrators more potential targets.

Growing Risk Awareness

There has been more media coverage in recent times surrounding data breaches and high profile cyber security cases which has increased organisation's awareness of the potential risks posed to their businesses. A recent Telstra research exercise showed that 36% of Australian respondents had implemented cyber-awareness programs. This growing awareness is leading to a more wide-spread adoptions of frameworks, risk assessments, security audits etc.

Increasing Regulation of Cyber Risk

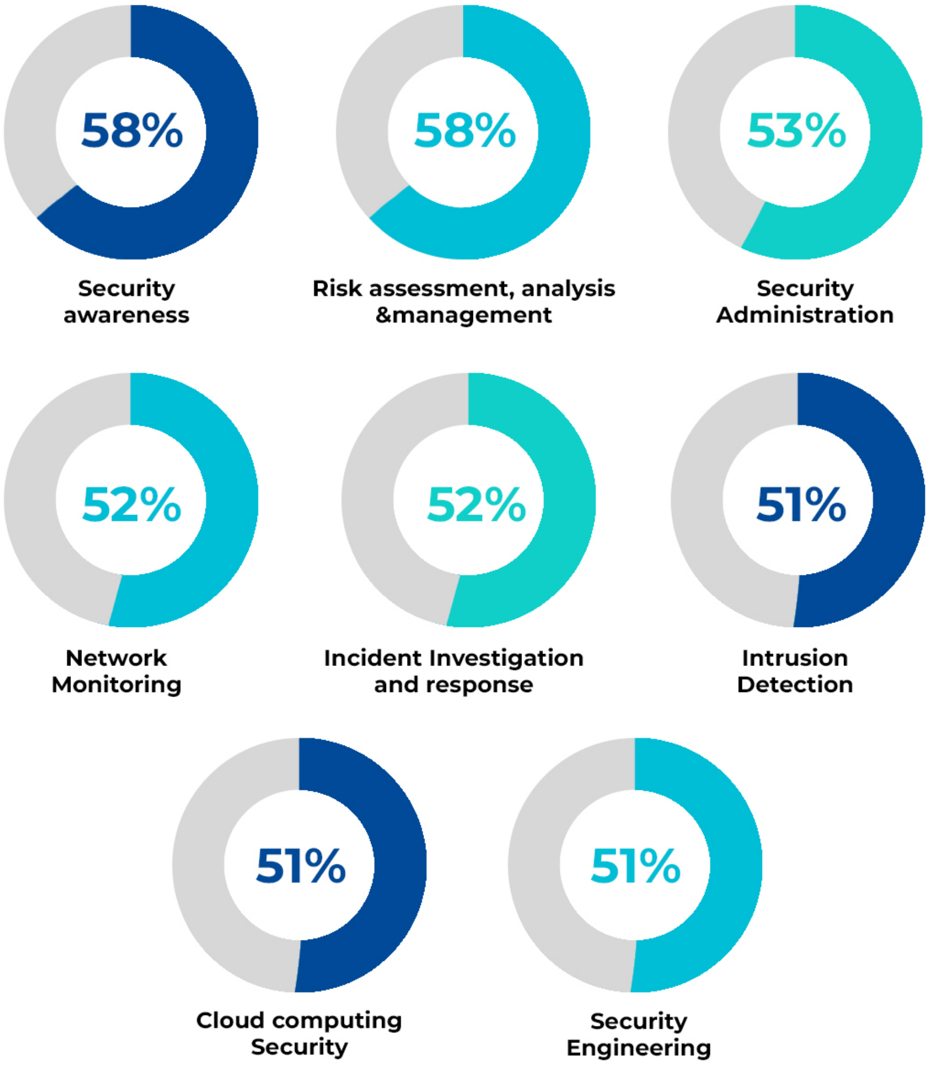
Many government organisations worldwide are issuing laws to ensure organisations are bettering their cyber-security controls. The new data breach laws in Australia are a great example, and similar laws will almost certainly lead to higher demand for new cyber security products and services.

Where to focus

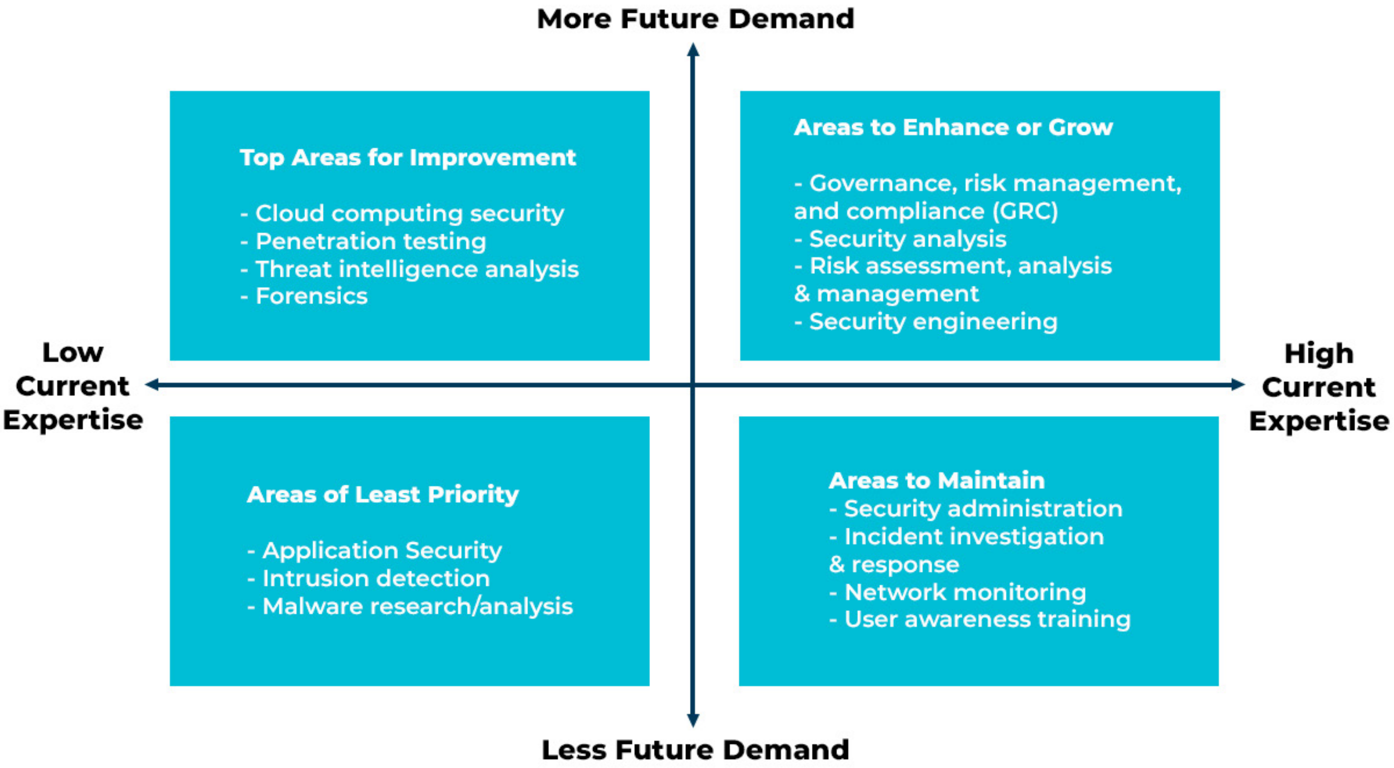
The International Information System Security Certification Consortium revealed the 8 areas of focus that cyber security professionals believe are the key components of remaining competitive in their field. At the top of the list sits Security Awareness and Risk Assessment, Analysis and Management skills.

Top Needed Cybersecurity Areas of Expertise

Showing % saying 'Critical'



Further, they asked the experts where they thought future demand would be in the industry and thus what they would need to upskill in. They charted where security experts identified low level of current expertise for improvement as well as the areas that would need to be maintained or enhance. The top skills that were predicted to be in high demand in the future but with little skill capability currently were the areas of cloud security, penetration testing and digital forensics. Experts also predict that areas such as governance, risk and security analysis, and security engineering would stay highly relevant in the future.



More Future Demand

Top Areas for Improvement

- Cloud computing security
- Penetration testing
- Threat intelligence analysis
- Forensics

Areas to Enhance or Grow

- Governance, risk management, and compliance (GRC)
- Security analysis
- Risk assessment, analysis & management
- Security engineering

Low Current Expertise

High Current Expertise

Areas of Least Priority

- Application Security
- Intrusion detection
- Malware research/analysis

Areas to Maintain

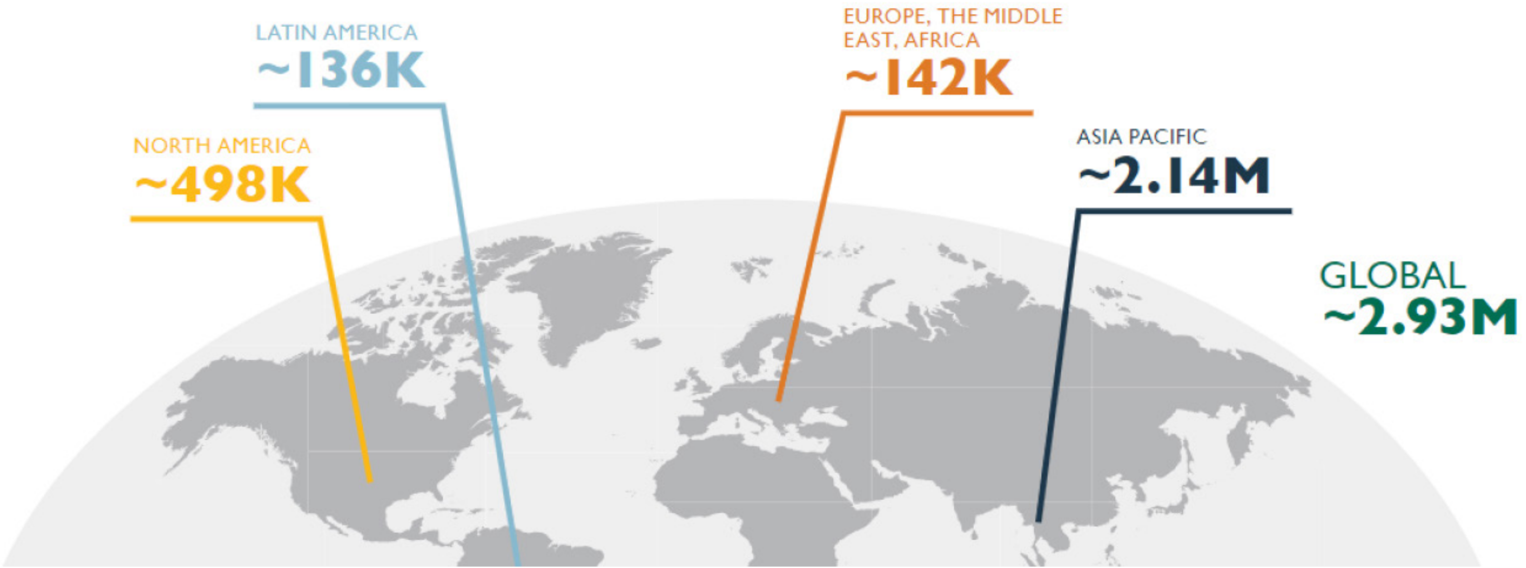
- Security administration
- Incident investigation & response
- Network monitoring
- User awareness training

Less Future Demand

Cyber Security Skills Shortage

According to the International Information System Security Certification Consortium there is a massive shortage of cybersecurity professionals across the globe – reaching nearly 3 million. In their 2018 Cybersecurity Workforce Study they polled 1500 security and IT professionals across North America, Latin America, APAC and Europe to explore the trends within the cybersecurity skills gab.

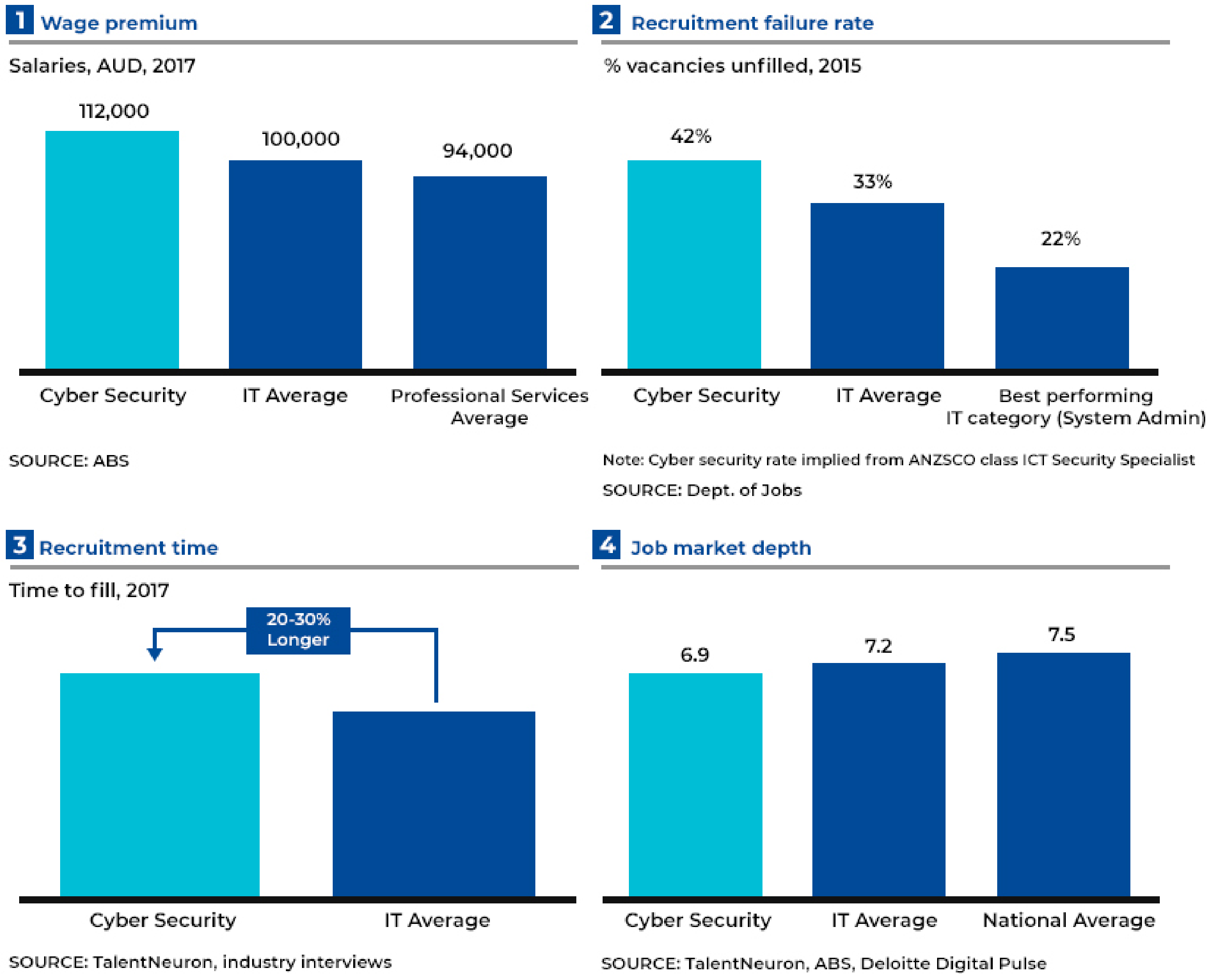
Gap in Cybersecurity Professionals by Region



This shortage of 3 million across the globe, is directly effecting markets everywhere. In Australia the shortage is estimated to be costing the nation $400 million through lost revenue and wages according to an AustCyber analysis. There is an estimated shortfall of approx. 2300 workers in the industry, and it is likely Australia will need a further 17,600 more workers by 2026.

Cyber security roles are increasingly difficult to fill; according to data from the Department of Jobs and Small business 42% of security focused roles went unfilled, and when they were filled it took almost 30% longer to find the right candidate. With this shortage there is also a premium on cyber security roles, costing organisations an average of $12,000 more than other IT roles.

Figure 21 - Skills shortage indicators in cyber security



1 Wage premium

Salaries, AUD, 2017

SOURCE: ABS

2 Recruitment failure rate

% vacancies unfilled, 2015

Note: Cyber security rate implied from ANZSCO class ICT Security Specialist

SOURCE: Dept. of Jobs

3 Recruitment time

Time to fill, 2017

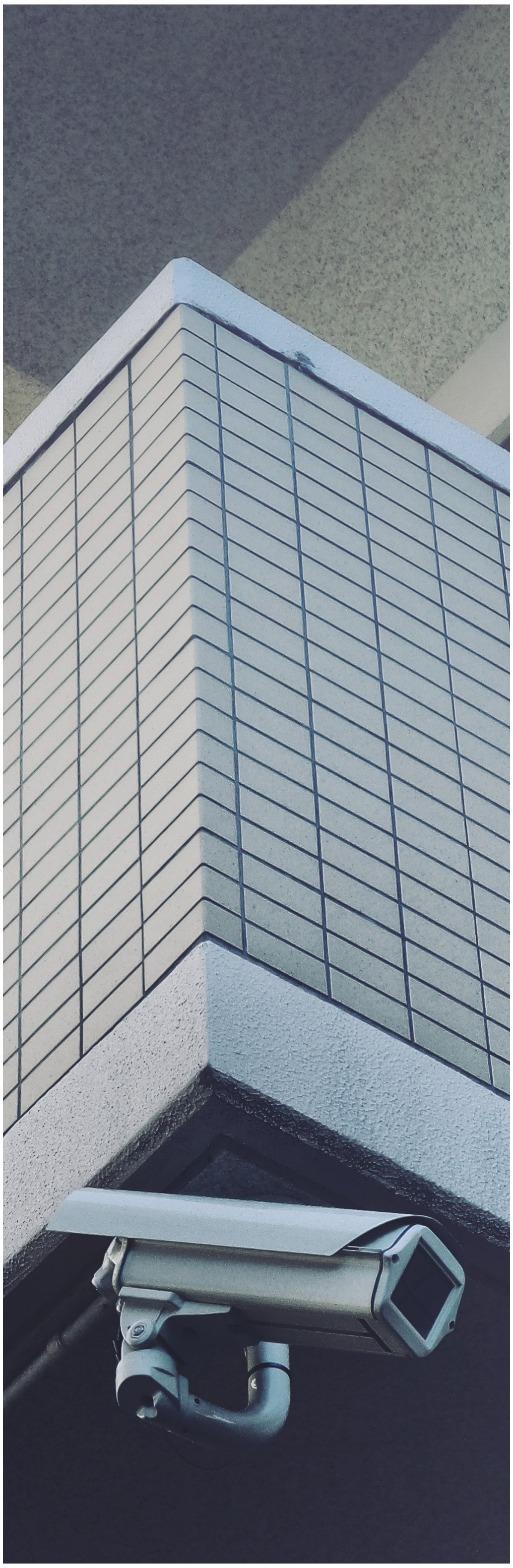
SOURCE: TalentNeuron, industry interviews

4 Job market depth

SOURCE: TalentNeuron, ABS, Deloitte Digital Pulse

Cyber Security Groups and Associations

AISA – Australian Institute of Cyber Security (https://www.aisa.org.au/)



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 3500 individuals and corporate sponsors 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. Their broad membership base consists of information security professionals from industries such as finance, education and government. Their members come from diverse backgrounds; ranging from company directors and managers, information security-related professionals, to lawyers, risk professionals, architects and highly-skilled technical specialists.

AWSN – Australian Women in Security Network

Australian Women in Security Network is open network of people of different backgrounds, experience, qualifications, age and gender who share a common interest in security. They aim to connect women in security across Australia and abroad, as well as supporting women already within the security industry to stay and grow. Further they aim to inspire the next generation and interested individuals to pursue a career in security.

AIIA – Australia Information Industry Association (https://www.aiia.com.au/about-us)

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity. The AIIA has a number of speciality interest groups, including cyber security, and run a number of great events year round.

Want to find out more? Let's chat.

ADELAIDE

Level 10,
26 Flinders Street
Adelaide, SA 5000
Australia

+61 (08) 8228 1555

BRISBANE

Level 21, Central Plaza 2
66 Eagle Street
Brisbane, QLD 4000
Australia

+61 (07) 3221 3333

CANBERRA

Level 2, Equinox 4
70 Kent Street
Deakin, ACT 2600
Australia

+61 (02) 6285 3500

MELBOURNE

Level 8, Rialto North
Tower
525 Collins Street
Melbourne, VIC 3000
Australia

+61 (03) 9602 4222

PERTH

Level 5,
150 St Georges Terrace
Perth, WA 6000
Australia

+61 (08) 9221 3300

SYDNEY

Level 9,
201 Elizabeth Street
Sydney, NSW 2000
Australia

+61 (02) 9223 9855

AUCKLAND

Level 4
5 High Street
Auckland, 1010
New Zealand

+64 (09) 281 4150

WELLINGTON

Level 3
Central on Midland Park
31 Waring Taylor Street
Wellington, 6011
New Zealand

+64 (04) 499 1200

Get in touch

Talent
Level 21, 66 Eagle Street
07 3221 3333

Find us online

www.talentinternational.com
www.linkedin.com/company/talent-international/