Talent

Cybersecurity Hiring Market Snapshot

Cracking the code to navigating the cybersecurity hiring landscape

october 2023

insights report _ cybersecurity

Contents

Cyber defences are needed.

Are you ready?

Cybersecurity is the hottest topic of 2023. With cyberattacks on the up, companies are recognising that now, more than ever, securing their systems needs to be a top priority. At present, there are over two million cyberattacks recorded per year, and by 2025, these attacks are estimated to have a global cost of $10.5 trillion – a significant increase from the $3 trillion reported in 2015.[1] Looking at 2023, cyberattacks have already increased by 7% in the first quarter of the year compared to the same period the year prior, with 1 in 31 global companies experiencing a ransomware attack per week during this time period.[2] This highlights the growing need for cybersecurity solutions, and with companies increasingly investing in security projects to protect against cyber criminals, the right tech talent is needed at the helm.

However, talent shortages are making things difficult. It's estimated that there is a shortfall of 3.4 million cybersecurity candidates globally.[3] A global survey has also highlighted that 57% of cyber professionals feel that a shortage of cybersecurity skills has had an impact on their company.[4]

So, what does this mean for you as a cyber professional? And what if you're a hiring manager looking to secure this talent for your business? Here at Talent, we work with businesses with a varying range of needs in this space and understand the challenges that we are all facing as companies and individual contributors. We've been working with cybersecurity professionals for many years now, connecting top talent with leading companies to drive significant tech transformation.

In this report, you will find exclusive insights from our recruitment experts and cybersecurity clients, highlighting what you can do, either as a cyber professional or employer, to get ahead in the market. We hope you find these insights invaluable in navigating the current hiring landscape.

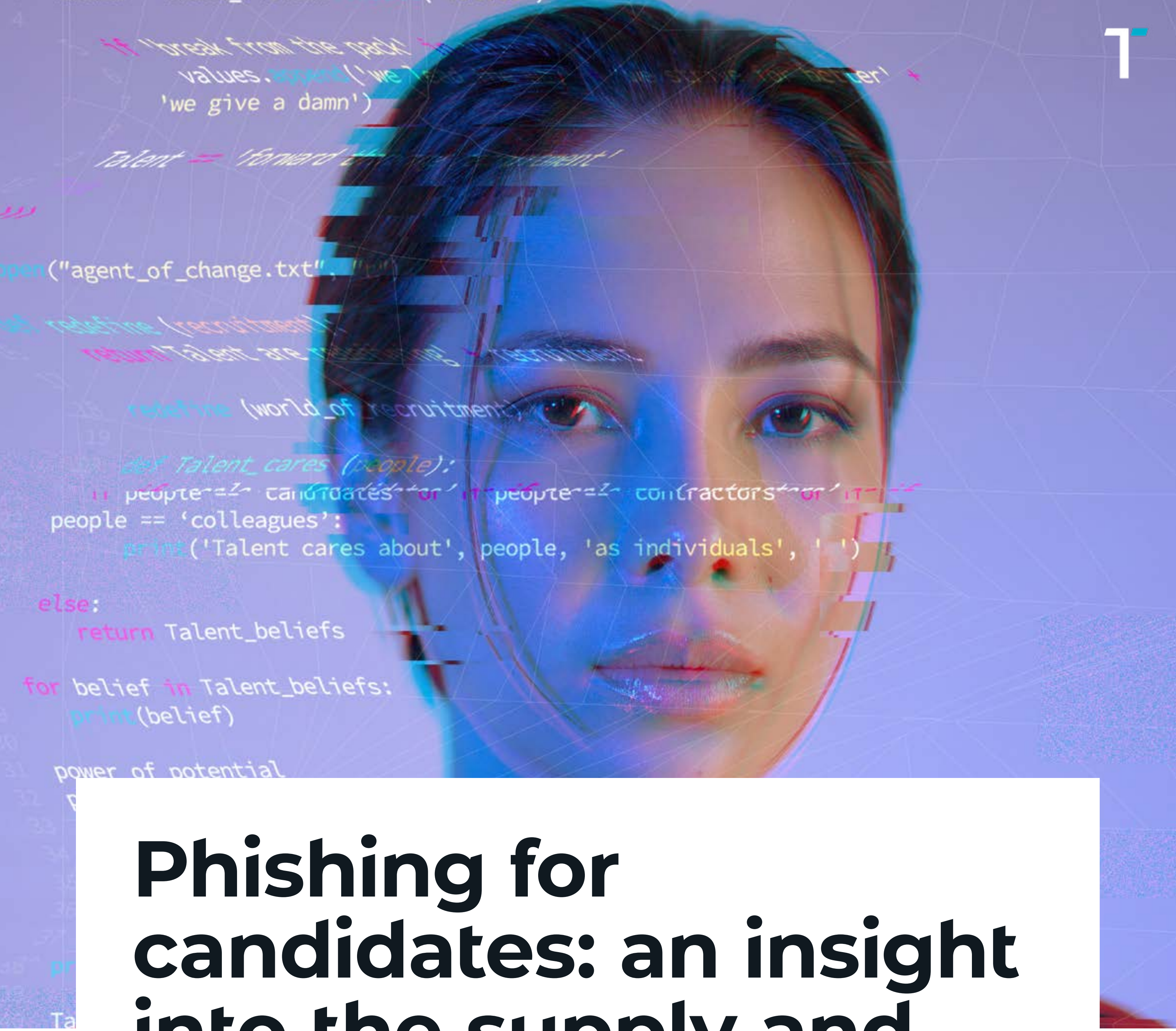
Mark Nielsen
Global CEO - Talent

Before you read on

The clients we interviewed as part of this report spoke to us under the condition that they remain anonymous.

This anonymity meant they could speak freely, sharing exclusive insights and predictions that they otherwise may not have been willing to disclose.

These experts have allowed us to go beyond the WAF (Web Application Firewall) to access one-of-a-kind insights that are so valuable, we just might need to encrypt them.


if "break from the pack"
values.append('we ... er'
'we give a damn')
Talent == 'forward ... ment'
open("agent_of_change.txt", "r")
redefine (recruitment)
return Talent are ...
redefine (world_of recruitment)
def Talent_cares (people):
if people == 'candidates' or if people == 'contractors' or if
people == 'colleagues':
print('Talent cares about', people, 'as individuals', '')
else:
return Talent_beliefs
for belief in Talent_beliefs:
print(belief)
power_of_potential

Phishing for candidates: an insight into the supply and demand of top talent

As cyber threats only become more prominent and complex, businesses across the globe are under pressure to lock down their systems and build a strong defence against attack. But none of this is possible without cyber warriors leading the way – those top security professionals who know their vishing from their phishing and are always one step ahead of malicious players.

What to expect

As an employer, you want those candidates with the technical capability to protect and defend – think, those who can build a honeypot that will take down cyber criminals within seconds. As a candidate, you want to work for those companies where you have the chance to participate in important projects that will take your career to new heights - after all, in a Talent survey of over 500 tech candidates, 85% said the opportunity for exciting and meaningful work matters most to them when looking for job.

So, what do you need to know when it comes to navigating the hiring market? Here's a look into what to expect:

First things first, why is demand so high?

Our Talent cybersecurity recruitment expert, Elliott Howard, observes that recent cyber breaches have been the catalyst for the explosion in demand for security talent "There have been supply and demand issues for cyber resources for a number of years, and the recent high-profile cyber incidents have further exacerbated this. Demand from our clients has definitely increased as they look to build up their existing cyber teams and defences."

Cyber experts are in short supply

Research has revealed that 60% of global IT and cybersecurity leaders struggle to hire qualified cybersecurity candidates in the first instance, while 52% struggle to retain these professionals once they are on board.[5] An Information Systems Audit and Control Association (ISACA) 2022 cybersecurity report also notes that sourcing is slow. Globally, 63% of companies have unfilled cybersecurity positions and 1 in 5 cite that it takes over 6 months to source relevant cybersecurity candidates for these roles.[6]

Qualified applicants are few and far between

Appropriately qualified cybersecurity candidates are hard to come by across the globe. In Australia and New Zealand, 52% of business leaders feel that cybersecurity job applicants aren't appropriately qualified[7] and it's a similar story in India where 59% cite that less than half of candidates have relevant qualifications.[8] A Cyber Services Manager at an Australian consultancy firm, notes "we tend to get a reasonable number of [cybersecurity] applicants but very few of those applicants are up to scratch. Some have far too little experience." An Information Security Governance Manager at a major bank also comments that "although increased recruitment is occurring across the board for cyber professionals, the demand for candidates with appropriate qualifications appears to be far outweighing the actual supply we are currently seeing in the market."

> **The demand for candidates with appropriate qualifications appears to be far outweighing the actual supply.**

Certifications are sought after

So, what do relevant qualifications look like? Research from the US has highlighted that several certifications are sought after by employers. In the top spot is Certified Information Systems Security Professional (CISSP) with over 183,000 US cybersecurity job listings citing this as a requirement. This is followed by Certified Information Systems Auditor (CISA) with in excess of 49,300 jobs noting this as a necessity, Security+ with over 20,700, and Certified Ethical Hacker (CEH) with more than 20,200.[9] An Information Security Governance Manager at a Talent banking client, notes that when it comes to hiring, "where we can see that candidates have begun a process of upskilling themselves, for example taking classes in Security + or are seeking to complete the CISSP or CISM exam, it is looked upon favourably."

Employers are considering new pathways

65% of IT business leaders in an Australian survey cite that a shortage of tech skills in their company is one of the main threats to their business, and resultantly 80% of these businesses are reskilling their employees into tech professionals.[10] One study has highlighted that those in administration and business support roles, warehousing and transportation positions, and those making a return to work after a significant period of leave, are assisting companies in filling tech skills gaps, with 41% reskilling into IT technician roles, 36% into cloud computing, and 36% into data analysis.[11] Professionals already skilled in tech are also increasingly considering upskilling and reskilling opportunities. Our cyber recruitment specialist, Elliott Howard, observes that a number of tech professionals are deciding to launch a career in the cyberspace, "Those in network engineering and network security roles are pivoting into cybersecurity; software developers with a strong security mindset are finding pathways into application security, transferring their coding skills between roles; and those in helpdesk, desktop support, and system administration positions who might be using Active Directory, can leverage those skills to make the move into UAR (User Access Reviews) / IAM (Identity Access Management) and Cyber Engineering." With the shortage of cybersecurity professionals only growing, reskilling is one answer to this challenge.

Seniors and specialists are in demand

When it comes to the hardest roles to hire for, our clients have shared their insights. A Cybersecurity Architect Manager from an IT services firm comments that "Senior and specialist cybersecurity roles are the hardest to fill. Seasoned professionals with a good blend of technical skills, commercial exposure, and good business acumen are highly desired." So, which of these roles are employers in need of most? "A few of the 'unicorns' in the market who are in a position to request higher wages include encryption specialists, 'cleared' senior security architects, and identity specialists (full lifecycle, not just Active Directory)". A Head of Digital at a retail client also notes that they are seeking to hire "Cyber Architect and Cyber Consultant professionals who possess technical depth and are able to consult and talk business risk to the internal stakeholder. These are quite senior roles which I see are in short supply within the market".

> **Seasoned professionals with a good blend of technical skills, commercial exposure, and good business acumen are highly desired.**

What about junior and mid-level candidates?

Employers aren't only looking for senior candidates - those with cybersecurity skills at all levels are sought after. A Head of Information Security at an insurance company shares "If I'm hiring tomorrow, it'll be a junior / mid-level person with a couple years of technical experience with the right attitude and mindset. Good generalists are hard to come by." This is a sentiment shared by a number of our clients, however, the shortage of cybersecurity candidates has meant that...

Salary expectations are high

Due to the short supply of cybersecurity talent, especially for senior roles, cyber professionals are seeking significant salaries. A Cyber Services Manager at a cyber consultancy shares that "Hiring for senior and / or management positions is difficult. In this space, experience is critical and there are even fewer genuine candidates to

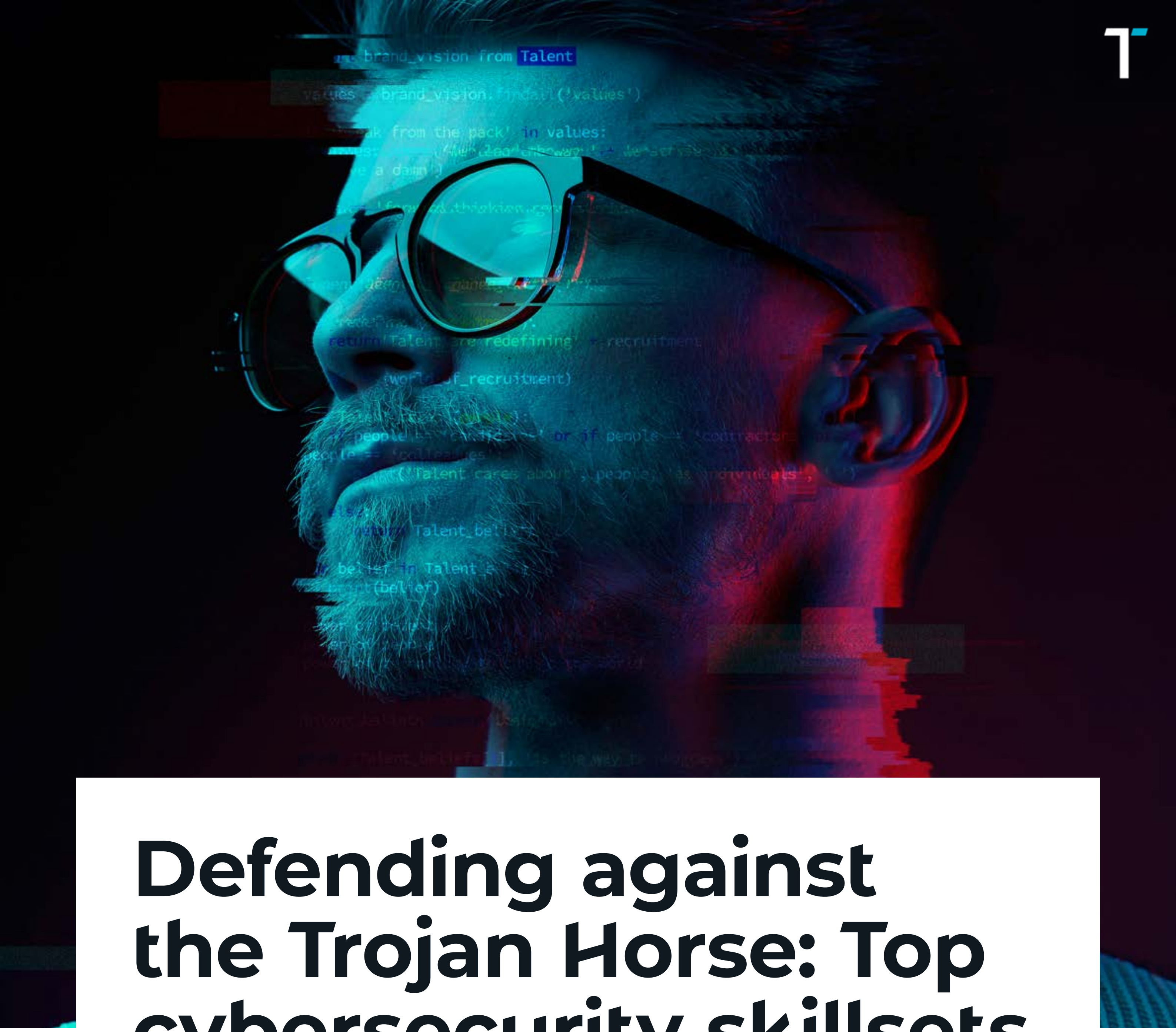
pick from. Those that are worth hiring are commanding quite high salaries and rates, and will likely have more than one organisation ready to snap them up." However, it's not only the senior professionals who are raking in the big bucks.

According to our cybersecurity recruitment expert, Elliott Howard, large consultancy firms and banks rolling out cyber graduate programs to grow internal teams, have had a strong impact on salary expectations. "While these programs have had a positive impact in increasing the pool of cyber candidates in the market, they have also resulted in candidates with only a couple years of industry experience asking for very high salaries which does not correlate to their experience. However, strong competition for cyber resources has meant that these less experienced candidates are sometimes able to attract the higher salaries and rates which further distorts market rates. This has resulted in enterprise-sized companies with large cyber teams and strict salary bandings struggling to match these salaries. They have therefore been unable to attract candidates, resulting in vacancies and extended periods of time to recruit."

Our cyber consultancy client shares this view, "Currently, I lead a team of level 1 and 2 security analysts and over the past 6-9 months I've had to hire. Given what we do, we tend to look for entry to mid-level experience to fill these roles, and cost is a big factor. What I've found is that those entering the market with little to no experience (or at least relevant experience) are commanding more in terms of salary. This is putting pressure on the profitability and competitiveness of the services we deliver."

With demand only growing for cyber talent as security threats loom, which skillsets are needed more than ever?

We delve into it.


brand_vision from Talent
values = brand_vision.findall('values')
from the pack' in values:
return Talent are redefining recruitment
(world_of_recruitment)
Talent cares about', people, 'as individuals'
Talent_beli
belief in Talent
(belief)

Defending against the Trojan Horse: Top cybersecurity skillsets to protect against attack

As cybersecurity threats become more sophisticated, companies increasingly need to stay one step ahead of criminals. However, this isn't possible without strong teams well-equipped with the latest skills and knowledge.

So, just like the latest software, it's time to run an update.

Top skills

If you're a candidate, taking note of your current capabilities and skilling up in high demand areas will not only ensure you're staying ahead of threats and protecting company data and systems, but will also open the door to new career pathways for you. If you're an employer, ensuring your security teams possess the right mix of technical and interpersonal skills is essential to ensure any vulnerabilities are strengthened up and you have a solid team who can spot a Trojan Horse a mile away.

So, which cybersecurity skillsets are in highest demand? We break into it:

Cloud Computing Security

Offensive Security

Security Operations

Artificial Intelligence

Cloud Computing Security

As cloud applications are increasingly relied upon with the growth of remote and hybrid work, the threat of cyberattacks is ever present. As a result, cloud computing security skills are highly desired. In a global survey by cybersecurity company Fortinet, 50% of companies are looking for cloud security specialists, yet this talent is in short supply. 57% of IT and cybersecurity managers have noted that cloud security roles are the most challenging to fill.[5] One of Talent's clients, an Information Security Governance Manager from a major bank, notes that "as more organisations are migrating applications and data to the cloud – they face new challenges in securing their cloud environments. As cloud security is a niche set of skills, I believe many organisations will look to offer greater opportunities to upskill their employees in this specific area of cybersecurity."

> **50% of companies are looking for cloud security specialists, yet this talent is in short supply.**

Security Operations

Endpoint security and security operations center (SOC) skillsets are highly sought after, with 42% of global companies seeking to hire Security Operations Analysts, yet 50% citing difficulty in recruiting these professionals.[5] According to our Sydney cybersecurity recruitment expert, Elliott Howard, SOC roles top the list when it comes to professionals in demand, "Some of the cybersecurity roles most in demand by our clients are Cyber Engineers (SOC, Cloud Security and DevSecOps) GRC Consultants, and Cyber Architects."

Offensive Security

When it comes to cybersecurity, it's not only about building a strong defence - it's just as important to construct a strong offensive strategy to stay ahead of cybercriminals. Shoring up systems by proactively searching for vulnerabilities is currently a key focus area for companies, with penetration testing and threat intelligence experts in high demand. According to a 2023 survey, 94% of cybersecurity professionals cited that penetration testing was either somewhat important or important to their company's cybersecurity strength. However, 63% of survey respondents noted that hiring enough skilled professionals to carry out penetration tests was their top challenge when implementing a penetration testing program in their company.[12] A Cyber Director at a Talent government client also notes that they are in search of tenured professionals with offensive security skillsets, citing that they are looking to hire "Offensive Security and Cyber Threat Intelligence Analysts including threat modelling, with 10 years' experience and certified OSCP, GPEN, GCTI".

Artificial Intelligence

As AI takes off, the need for professionals who understand the ins and outs of this technology and can remain ahead of cybercriminals who are leveraging its capabilities, is higher than ever. With the global 'AI in cybersecurity' market valued at over $10 billion in 2020 and projected to reach $46.3 billion by 2027[13], companies are increasingly integrating AI into their cybersecurity operations and need skilled professionals to lead the charge. One Talent client, an Information Security Manager from a major bank, shares that they are in need of "experts with Artificial Intelligence skills, where AI is used for SOC", however, they note that this skillset is challenging to hire for.

```
   values.app

Talent ==
>>>

f = open(

def                ent):
   return             recruitment

redefine (wor      ruitment)

def                le):
   if people       tes or people =
      print(          , peop

   else:
      return        liefs

for belief in       eliefs:
   print(beli

power of pote
power of people
power of technology to change the world
>>>

Talent_beliefs.append(   )

print (Tale
```

Beyond technical skills… it's time to talk the talk

Cybersecurity professionals who possess both technical AND non-technical skills are highly sought after. A Cybersecurity Architect Manager in the IT services space, shares that "candidates who have the technical acumen are a plenty, however the ability to communicate in literal and verbal mediums, combined with a good set of interpersonal skills, differentiates the good from the not so good candidates."

> **Candidates who have the technical acumen are a plenty, however the ability to communicate… differentiates the good from the not so good.**

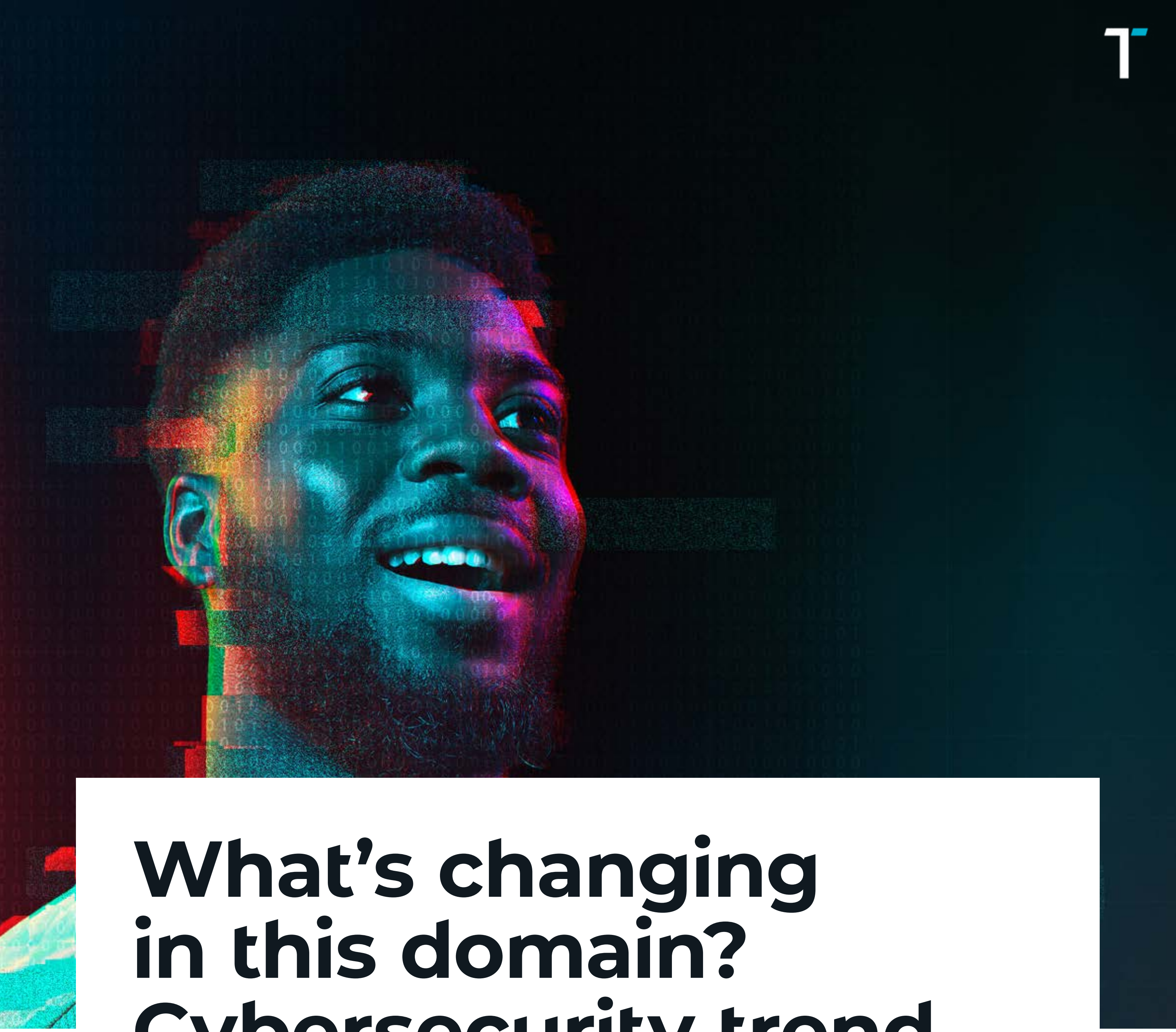
Another client, a Cyber Manager at a Financial Services company notes "I look for attitude, proven communication skills, and being able to bridge the tech and human components of what we do. Everything in cyber, as with most areas, requires collaboration and results from other teams. A great communicator will achieve more than a brilliant tech in some cyber roles."

Strong communication and advisory skills are also an imperative for cybersecurity experts when engaging with clients or a company's executive team. An Information Security Manager at a major bank, notes that they are in search of security candidates who are "capable of successfully communicating with senior management to convince them to invest in security", while our IT services firm client shares that they are in search of professionals who are "able to present, pitch, and articulate their proposal or opinion to key stakeholders to provide value to the industry".

This is a sentiment shared by companies across the board when hiring cybersecurity professionals. Talent Sydney cybersecurity recruitment expert, Elliott Howard, observes "Our clients are typically seeking candidates with a mix of strong technical skills along with excellent communication and consultative skills to be able to work closely with business stakeholders and explain threats and trends in plain terms. Interpersonal skills are more challenging to identify on a resume which is where engaging with a specialist technology recruitment agency can be beneficial"

However, those who possess these strong communication skills can expect to be in a stronger bargaining position when it comes to salary. A Cyber Services Manager at a cyber consultancy cites that their preference is "to hire those who are a bit consultative in nature with a good degree of interpersonal skills in managing clients. Such candidates are certainly in short supply, but if you find one, it's often worth paying that little bit extra given the benefits they can provide."

As new technology enters the market and cybercriminals leverage this for increasingly sophisticated cyberattacks, the skills landscape will continue to shift. So, what can we expect in the cybersecurity space over the next 12 months and beyond? We explore what's next.



What’s changing in this domain? Cybersecurity trend predictions

The cybersecurity space is constantly evolving. With the rise of AI, increasing reliance on Cloud, and the ever-growing Internet of Things, vulnerabilities are popping up left, right and centre. With deepfakes taking hold and cyber criminals leveraging AI to impersonate business leaders in sophisticated vishing attacks, threats are becoming harder and harder to spot. So, what's on the cards for cybersecurity in 2024 and beyond?

What's in store?

What's in store for cybersecurity over the next 12-24 months? These are the top predictions from our clients and recruitment experts.

✓ Regulation will increase

To protect against risk, our cybersecurity clients predict that there will be greater regulation for companies when it comes to cybersecurity. Across Australia, a Head of Information Security at an insurance firm foresees that there will be "Greater scrutiny from regulators (APRA, ASIC) for regulated entities", while a Head of Information Security at another insurance company expects "increased regulation from APRA and regulatory bodies i.e. CPS 230."

AI will present new risks

With the explosion of ChatGPT and other AI tools, comes a whole new ball game of cyber threats. Think – cyber criminals leveraging AI technology to generate convincing phishing emails, or the potential of using these tools to generate automated malware. Resultantly, our Head of Information Security client in the insurance space foresees the growing need to "defend against the increasing volume and sophistication of AI-enabled threats" while a SOC Manager at a Digital Solutions client predicts that there will be "more sophisticated attacks across the board as AI really takes hold". A Cyber Services Manager at a cyber consultancy also cautions "We'll see a lot more in the [AI and Machine Learning] space as new ideas off the back of these concepts emerge and mature. What we need to really watch for is how adversaries use these same concepts. As always in the information security space, attackers tend to harness new technologies for evil before we're ready to defend against them."

Digital fraud will rise

The rapid advancement of technology comes with both benefits and risks. An Information Security Manager at a major bank anticipates that we will see an "increase of digital fraud due to criminals being able to use the capabilities of artificial intelligence, deep-faking, and super computing". This is an issue which permeates through the Financial Services space, with an Information Security Lead at an insurance provider foreseeing that the next 1-2 years will involve a "focus on dealing with AI-powered attacks and the capability of organisations to be on top of these. Organisations wouldn't be able deal with these standalone and there would be an emergence of a more collective effort between companies."

Third parties will be reassessed

In a bid to secure company systems, many turn to third party solutions for their cybersecurity management. One Talent client, a Cyber Manager at a financial services company observes that “third party data breaches are making organisations reassess what they are willing to outsource and / or what data their third parties need”, while another, an Information Security Governance Manager at a major bank, foresees that there will be “increased awareness and focus on supply chain risk and ensuring that a ‘commensurate with risk’ approach is taken for organisations’ 3rd and 4th parties.”

Security will receive more investment

Cybersecurity is the hottest topic of the moment, but there is still some way to go when it comes to business investment in this space. A 2022 survey revealed that only 36% of medium-sized businesses and 42% of larger companies consider cybersecurity a top budget priority in the US, and it appears things are similar across the globe.[14] In the coming years, an APAC Security Officer at an insurance client company, predicts that “Compliance and governance will continue to be a focus area. Hopefully with this, information security will not be seen as a domain under IT but will get more visibility from the business. With recent breaches, litigation, and the government's cybersecurity strategy, the board and executives may support the information security team more when it comes to understanding organisational risks, and allocating budget, including uplifting existing capability.”

Employee training will be a priority

With 88% of company data breaches attributed to employee error[15], and social engineering attacks only on the rise – email-based phishing attacks have increased by 464% since the first half of 2022[16] – cybersecurity training for team members is a growing priority. With employees presenting a strong risk to a company’s overall security, think the recent MGM casino hack[17], companies are recognising now more than ever, that cybersecurity is everyone’s responsibility. Michael Megally, General Manager at Avec, Talent’s project delivery company, cautions that “Cybersecurity can’t all be left up to your IT team. You can build the biggest cyber defence in the background, but your people are your biggest vulnerability. Training your people is the biggest defence you can have.”

The emphasis on security is so strong that there’s increasing debate around whether those who fail phishing tests should be fired[18] - 39% of company decision-makers in the UK let go of employees who breached company security policy during the pandemic. [21] Resultantly, cyber training is on the up. Research has revealed that the global security awareness training market currently sits at approximately $5.6 billion in 2023 (up from $1 billion in 2014) and it’s predicted that this will exceed $10 billion annually by 2027.[19] 97% of companies in a 2022 survey also noted that they had implemented security awareness measures[20], and Clive Mathieson, Partner at Cato & Clive Partners, a PR and communications consultancy, has observed an increased investment in cybersecurity testing:

"The best-prepared organisations are conducting regular, full crisis scenario exercises. They are not cheap and can be a big investment in management time but they are incredibly useful for identifying gaps and issues that will hurt you in a real event."

Demand for talent will increase

Anthony Whyte, Talent Adelaide Managing Director notes "As well publicised, there have been numerous critical data breaches over the past 12 months. As a result, cybersecurity is now the number one most talked about topic in most, if not all, company board meetings.". Talent Brisbane Managing Director, Keith Dixon also observes that "with the recent security breaches experienced by major corporations, the demand for cybersecurity related skillsets has increased exponentially". And this isn't a topic that's going away anytime soon - as cyberattacks and data breaches continue to occur, companies are more determined than ever to protect their systems. A Head of Digital at a Talent retail client predicts that "Cybersecurity demand will increase even if IT budgets are maintained or decreased, and demand for cyber skills will intensify".

So, are you prepared?

It's clear that the threat landscape is evolving and the risk of cyber breaches is only growing, however protecting a company's systems can't all fall on the shoulders of a new cyber hire. Company-wide investment in cybersecurity is a must, and everyone has a role to play in preparing for a crisis.

Poor communication can spell disaster

As companies become more aware than ever of the reputational risks that arise with cyberattacks, they are increasingly attempting to get on the front foot to limit any potential brand damage. Clive Mathieson, Partner at Cato & Clive Partners, notes that "The recent run of cybersecurity incidents affecting major organisations has certainly focused the minds of boards and management on whether their own systems are robust and whether they are well prepared to respond to an incident. An important part of any response is having a clear communications plan, with the reputational damage caused by confused communications, particularly to customers, often greater than the impact of the incident itself."

Hire for a crisis

It's a great idea to consider hiring a communications professional with crisis comms skills to join your cyber response team or offer upskilling opportunities to your comms professionals to ensure they're armed and ready if a cyberattack were to occur. Mathieson's advice: "While training is critical, it's also valuable to have people who have been through the real thing - in communications and in the other key components of your response team, such as operations, IT and legal. When hiring communications personnel, look for some who have done more than marketing and publicity. Even if a past crisis did not go well, they will have learned an enormous amount about what to do - and what not to do. They can be a voice of reason."

Look externally

When it comes to hiring for these skills and experience, Mathieson suggests "If you don't have this experience in-house - and even if you do - it is worth building a relationship with external experts in cybersecurity and issues communications. Third parties can be invaluable in providing clear, unemotional advice to help a rattled organisation stay calm and make the right decisions. The better they get to know you and your organisation before a crisis, the more valuable they can be."

And finally, ensure everyone is involved

As the adage goes, "if you fail to plan, you plan to fail", and this certainly rings true when it comes to cybersecurity. Your people should be across your crisis plan and be ready to go when the going gets tough. Mathieson's suggestion? "In terms of getting your communications right in the heat of a crisis, the best advice I can give to any organisation is to make sure your people are familiar with your crisis communications plan before you're in a crisis. Everyone needs to know what needs to be done, what they are responsible for, where they need to go for information. If your people are flicking through the crisis communications plan for the first time in the middle of a crisis, you've wasted all your preparation and you're already on the back foot."

With the ever-growing focus on cybersecurity and the need for skilled talent to protect companies across the globe, what does this look like in different industries?

From Education through to Energy, we break into it.

import brand_vision from Talent
values = brand_vision.findall('values')
'break from the pack' in values:
values.append('we lead the way' + 'we strive for better'
'we give a damn')
Talent == 'forward thinking recruitment'
("agent_of_change.txt", "r")
def redefine (recruitment):
return 'Talent are redefining' + recruitment
redefine (world_of_recruitment)
def Talent_cares (people):
if people == 'candidates' or if people == 'contractors' or if
people == 'colleagues':
print('Talent cares about', people, 'as individuals', ',')
else:
return Talent_beliefs
for belief in Talent_beliefs:
print (belief)
power of potential
power of people
power of technology to change the world
Talent_beliefs.append('being different')

Locking down a defence: Industry sector insights

Protecting data and systems is an imperative across all industries and organisations, however some have been more affected than others. Here are the industries where cyberattacks are the most targeted and what they are challenged by most when it comes to securing their systems and finding top talent.

Education & Research

With significant digital transformation occurring in the education & research sector, this has made the industry a textbook target for cyber criminals. The increased uptake of Enterprise Resource Planning (ERP) systems, cloud platforms, and e-learning systems to manage student and faculty data and enhance the student experience, has resulted in a growing need to protect this information… and the numbers paint a concerning picture. The sector has experienced 2507 attacks weekly per institution in 2023, a 15% increase since Q1 2022.[22] As threats only grow in this space, the need for A+ cybersecurity talent only rises. According to LinkedIn, the higher education sector has seen a 41% increase in employment of professionals skilled in cybersecurity since September 2022 and the research sector a 31% increase. However, the education industry still isn't appropriately equipped to handle these threats – out of 17 major industries, education ranked last when it came to cybersecurity preparedness.[23]

> **The [Education & Research] sector has experienced 2507 attacks weekly per institution in 2023.**

Financial Services

Cyber criminals are attempting to cash in on the wealth of valuable data held by the financial services industry, particularly due to the explosion of e-banking and the stores of customer information these institutions manage. In 2022, the global rate of ransomware attacks in the sector sat at 55%, and this increased to 64% in 2023 - a significant jump from the 34% reported in 2021.[24] With cyberattacks affecting financial services companies far and wide, the need to protect systems and customer data is more important than ever – and the sector is banking on having the right people closing in on cybercrime: top talent. However, with the financial services industry losing out on candidates to industries that offer more competitive remuneration such as global tech providers or cyber consultancies, securing this talent isn't easy. Especially when the industry is already experiencing a significant candidate shortage – the finance and insurance industry in the US, for example, saw 168,000 cybersecurity job openings in 2022 with the country only having enough workers to fill 68% of open cybersecurity roles.[25] Over in APAC, Elliott Howard, Talent Sydney cybersecurity recruitment expert, shares that "while large enterprises such as financial service, telecommunication and consultancy organisations continue to grow their large, in-house cyber teams, we have certainly noticed an ongoing trend of cyber professionals moving from these organisations to join specialised cyber consultancy firms where remuneration is more competitive".

Energy

With the move to renewables, growth of GreenTech, and increasing digitalisation of the energy sector, it's no surprise that this industry is an increasing target for cybercrime. In 2022, 10.7% of global cyberattacks were experienced by the energy sector[26], with the average cost of a cyber breach in this industry sitting at $4.71 million.[27] Additionally, the International Energy Agency, an intergovernmental organisation dedicated to the research and analysis of the global energy industry, has indicated that organisations within the sector struggle to source and retain appropriate cybersecurity professionals to defend their companies against risk. Research by the agency has also highlighted that cyberattacks are the catalyst for spikes in demand for cybersecurity professionals, indicating a lack of long-term cyber strategy across the sector. However, people power is an issue: the global shortage of security professionals makes sourcing this talent a tricky task.[27]

Manufacturing

The growth of smart manufacturing and use of cloud technologies to generate efficiencies in the manufacturing process has resulted in the industry experiencing a significant share of cyberattacks. The sector recorded a 24.8% share of global attacks in 2022[26] indicating the need for significant investment in the cybersecurity space to mitigate risk. Resultantly, it's projected that cybersecurity investment within the manufacturing sector will reach $29.85 billion by 2027[28], with a strong investment needed in security professionals who can assemble strong system defences.

> **It's projected that cybersecurity investment within the manufacturing sector will reach $29.85 billion by 2027.**

Retail

Cyber criminals are bringing new meaning to the term 'click and collect'. Between 2021 and 2022, ransomware attacks increased by a significant 75% in the retail industry[25], emphasising just how much this sector can't afford to 'check out' when it comes to cyber crime. Handling stores of customer data, overseeing Cloud POS systems, and managing the supply chain, retail companies need to be prioritising cybersecurity to protect this endless aisle of sensitive customer and supplier information. Research, however, has revealed that for some, this is on the backburner - only 22% of retail companies are currently training their employees in cybersecurity.[26] 71% of retail IT and business leaders have also noted concern about the size of their digital attack surface. Taking stock of threats in the industry – credit card skimming and ransomware is rife in this sector – the need for skilled cyber professionals is stronger than ever. Yet, as is clear across all industries, it's a classic issue of supply and demand – there simply aren't enough cybersecurity professionals to protect against the growing threats thrown the retail industry's way.

Healthcare

With a shift to digital and e-health – think telehealth appointments, wearable technology, and electronic health records – the healthcare industry is not immune to the cyberattacks and viruses plaguing industries across the globe. Research has revealed that in 2022, healthcare organisations experienced 1,426 attacks weekly – a 60% increase since 2021. Q3 of 2022 also saw 1 in 42 healthcare organisations experiencing a ransomware attack.[27] Nathan Crawford-Condie, Client Services Manager at Avec, Talent's project delivery company, comments that "The number of ransomware threats are growing exponentially, and healthcare is over-represented in breaches, so is highlighted as an easy target for criminals. In a world where the likelihood of being a victim of cybercrime has moved from if to when, healthcare leads the pack.” Investment in cybersecurity, however, isn’t sufficient to develop a strong defence against attack. A 2022 survey by the Healthcare Information and Management Systems Society revealed that US healthcare organisations are spending 6% or less of their IT budget on cybersecurity and that finding the right people to place on the frontline is a tough ask. Sourcing top cybersecurity talent is a challenge due to limited budgets, a lack of qualified candidates, and an inability to offer competitive remuneration.[28]

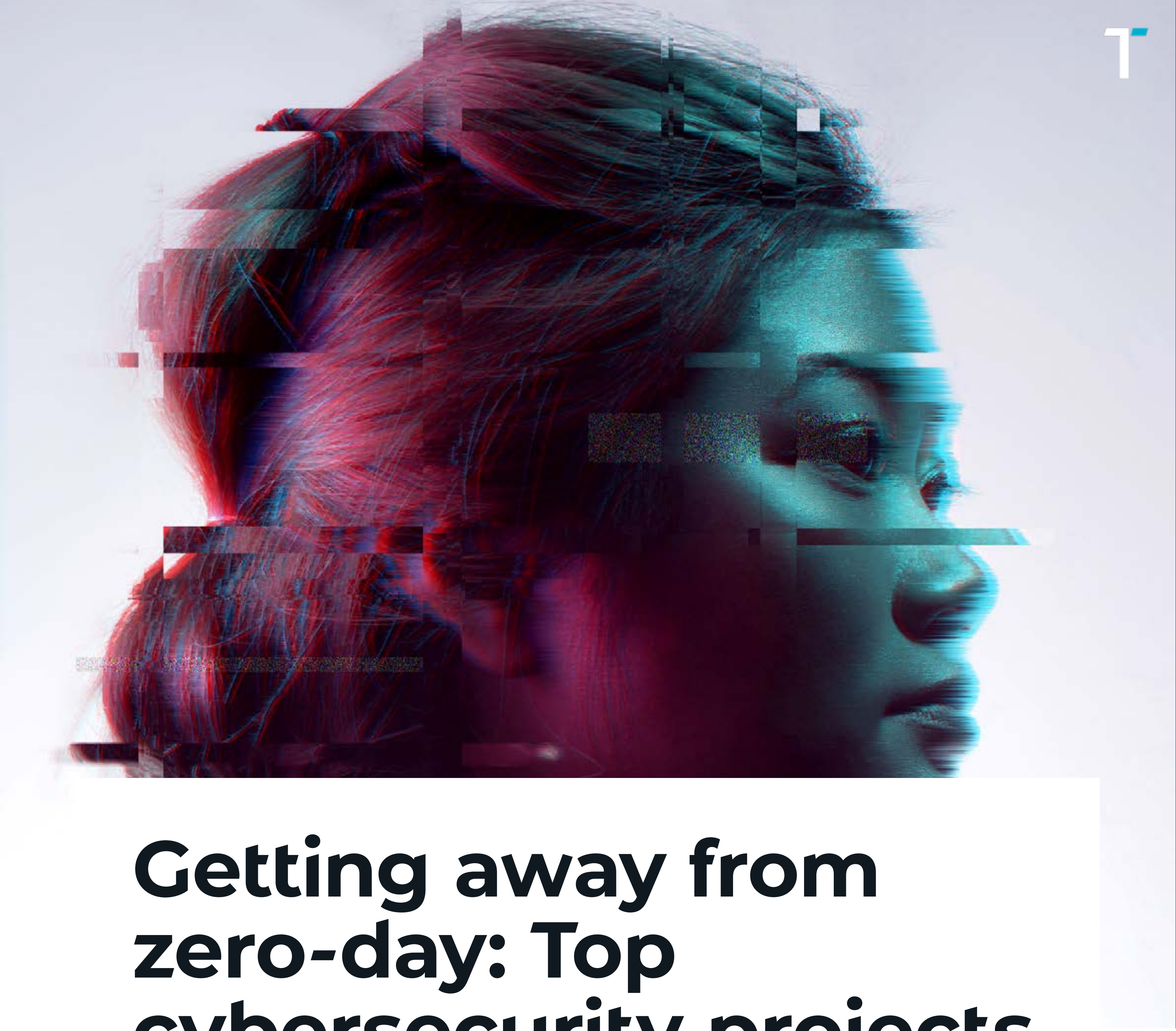
> **Healthcare organisations are spending 6% or less of their IT budget on cybersecurity.**

Government

With the rise of state-sponsored threat actors driven by political, financial and military aims, Government departments are more alert than ever when it comes to securing their systems and data from attack. Research has highlighted that cyberattacks in this sector increased by 95% in the second half of 2022, compared to the same time period the year prior.[29] However, the industry is struggling to develop a strong defence without the right people on board - insights from the US have revealed that there is a shortage of 36,000 public sector cybersecurity jobs across federal, state and local government.[30] Without the implementation of cybersecurity projects and qualified candidates protecting against everything from spyware to malware, global governments are at risk of data breaches that could have far-reaching implications.

Beyond industry, what are companies across the globe prioritising when it comes to cybersecurity? We explore this next.

```
f = open("agent_of_change.txt", "r")

def redefine (recruitment):
    return'Talent are redefining' + recruitment

redefine (world_of_recruitment)

def Talent_cares (people):
    if people == ‘candidates’ or if people == ‘contractors’ or if
people == ‘colleagues’:
        print('Talent cares about', people, 'as individuals', ' ')

    else:
        return Talent_beliefs

          Talent_beliefs:
```



Getting away from zero-day: Top cybersecurity projects

What are companies investing in when it comes to strengthening their cybersecurity defences and getting ahead of cybercriminals? We look into the top digital projects that are transforming the cyber space.

Global projects

Cyber threats are coming harder and faster, seeing companies across the globe focusing their efforts on shoring up their systems and protecting themselves from attack. Our cybersecurity clients in companies from retail through to banking, have weighed in on what their top priorities are for 2024:

- Reducing customer data footprint in core systems, to minimise impact in the event of a security breach
- SIEM/SOC capability update
- PCI-DSS gap remediation
- Identity lifecycle governance
- Security operation automation and orchestration
- Compliance and general posture maturity improvements
- Data leakage protection
- Security simplification
- AI and automation
- Monitoring of high risk suppliers i.e. third party risk
- Vulnerability management
- Identity and Access Management (IAM)
- Uplifting Essential Eight (E8) maturity

The most important project of them all? Getting everyone on board.

While it's often left to the IT team to combat cybersecurity issues and ensure teams remain vigilant about the ever-present threat of cybercrime, the truth is it's everyone's responsibility.

After all, a Stanford University study revealed that 88% of all data breaches are due to an employee mistake.[15] When it comes down to it, senior leaders and cyber professionals aren't the only ones that are responsible for locking down company systems and data - every project manager and team member needs to be responsible for the data security of their projects.

It is vital that every person onboarded to a project team understands potential security threats, is equipped with the tools on how to deal with them, and is aware of their own responsibilities when it comes to security. With proper training and understanding, every team member has the power to act as the first line of defence against potential cyberattacks.

We can support your team with cybersecurity in your projects by providing thought leadership and consultative services.

Learn more about what we can offer through our project delivery company, Avec.

Learn how we can help

brand_vision from Talent
brand_vision.findall('values')
(world_of_recruitment)
return Talent_beliefs
power of technology to change the world
talent_beliefs.append('being different')
print (Talent_beliefs[3], 'is the way to progress')

Breaking into your region: Global insights on cybersecurity

What are global companies investing in when it comes to cybersecurity, and what does the hiring market look like as a result? We delve into the top projects shaping the cybersecurity sphere and take a deep dive into what's happening in the hiring markets of each of the regions we operate in globally.

Australia

Across Australia, cybercrime is on the up. In FY22, the Australian Cyber Security Centre (ACSC) noted that it had received in excess of 76,000 cybercrime reports, an increase of 13% from the financial year prior. The majority of these incidents occurred across the following industries: the Commonwealth government at 24%, state and local government at 10%, health care at 9%, and information, media and telecommunications at 8%.[31] Digital transformation projects continue to be invested in across all industries, which pose increasing security risks for companies operating in these spaces. However, most Australian companies feel they are not prepared to handle a cyberattack – research reveals that 67% of IT leaders feel they are not appropriately equipped to quickly detect a data breach, while 75% cite that their company's data infrastructure is not sufficient to deal with ransomware attacks.[32]

> **By 2026 it is estimated that Australia will need almost 17,000 more cybersecurity workers to meet the country's needs.**

However, it's not only a lack of data infrastructure that's causing problems, a shortage of qualified cyber professionals is also impacting businesses across the country. According to AustCyber, by 2026 it is estimated that Australia will need almost 17,000 more cybersecurity workers to meet the country's needs[33], and this is only growing. The Australian federal government, for example, has invested $9.9 billion into a new cybersecurity program overseen by the Australian Signals Directorate (ASD). The Resilience, Effects, Defence, Space, Intelligence, Cyber and Enablers (REDSPICE) program intends to build Australia's cybersecurity strength and capabilities and will require 1,900 new technologists and cybersecurity professionals across the country and globe to support the project.[34]

Moves are already being made to meet the demand for top cybersecurity talent, with Australian education institutions enhancing their offering of cybersecurity courses and degrees, which could see a growing talent pipeline emerge in the cybersecurity space - it's estimated that the number of cybersecurity graduates could grow at 4x the current rate to reach 2000 per year by 2026.[33] The Australian Government Department of Industry, Science and Resources has also awarded up to $25.4 million of funding to 18 projects that will enhance the quantity, quality and diversity of the country's cybersecurity workforce through scholarships, paid internships, and mentoring projects.[35]

New Zealand

Cybersecurity attacks are having a significant impact on New Zealand. The country has experienced an average of 2,266 cybersecurity incident reports and $5 million of direct financial loss per quarter in 2023.[36] Cybersecurity threats are only on the rise, with phishing and credential harvesting seeing a 26% increase between Q1 and Q2 alone.[36] To combat growing cybersecurity risks, the government has invested $94 million since 2018 to improve NZ's cybersecurity defences and capabilities.[37] Delving further into this funding, the New Zealand Ministry of Defence has invested in a project to improve the NZDF's military cyber capability and protect its systems. This will involve uplifting its capability by the way of people, policies, technologies and processes.[38]

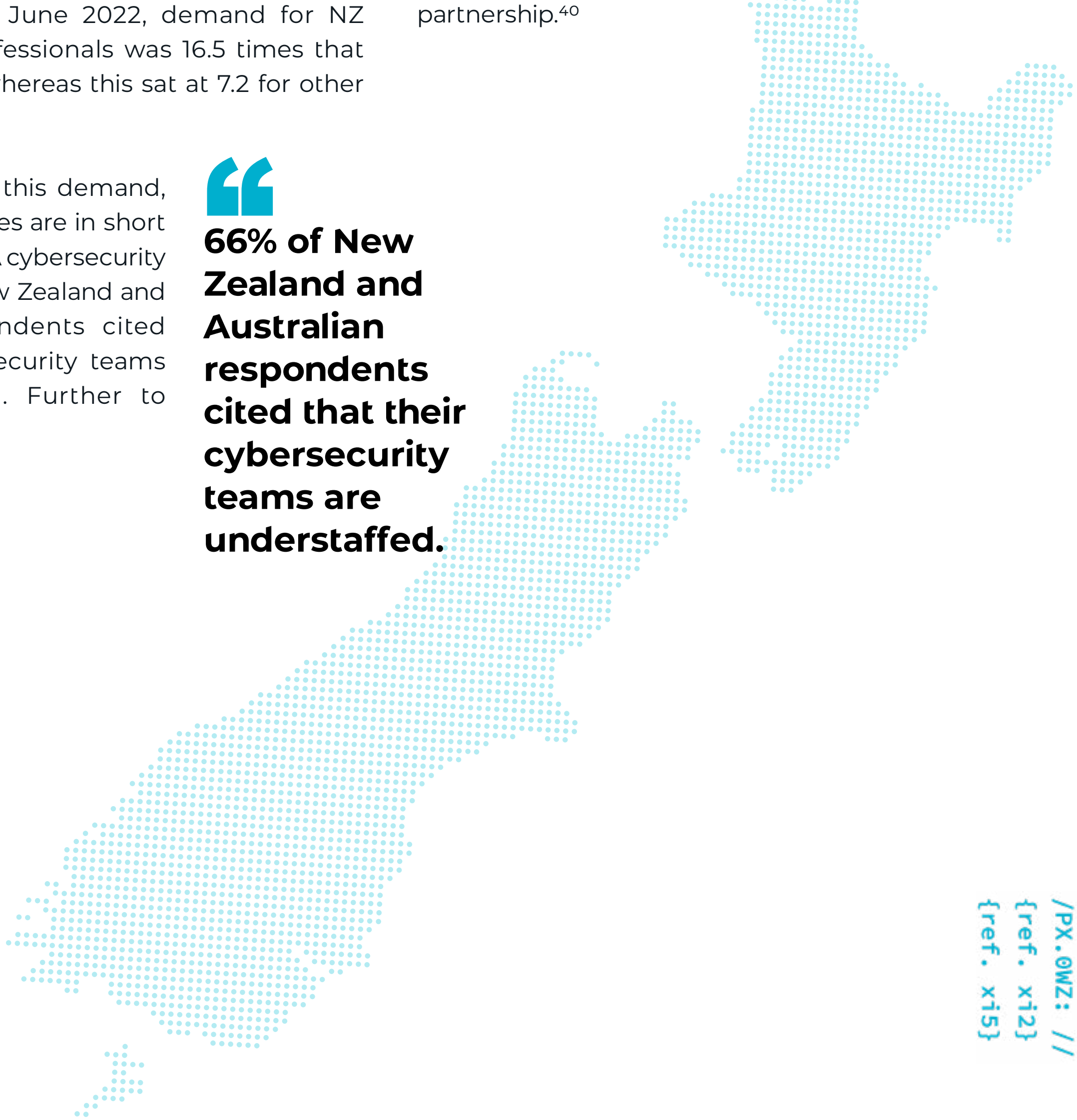
As a result, the need for cybersecurity professionals is higher than ever. Data from the OECD has revealed that demand for this talent has outpaced the growth of demand for other occupations – in June 2022, demand for NZ cybersecurity professionals was 16.5 times that of January 2013, whereas this sat at 7.2 for other professions.[39]

However, despite this demand, qualified candidates are in short supply. In an ISACA cybersecurity survey, 66% of New Zealand and Australian respondents cited that their cybersecurity teams are understaffed. Further to this, 59% noted unfilled cybersecurity positions in their companies, and in a bid to fill these vacancies, 52% cited that applicants are not appropriately qualified.[7]

> **“**
> **52% cited that applicants are not appropriately qualified.**

With a shortage of skilled security professionals, NZ organisations are looking to fill the gap through education. Vocational education provider, Te Pūkenga (New Zealand Institute of Skills and Technology), for example, has partnered with Microsoft, TupuToa (a Maori & Pasifika not-for-profit), and Te Whatu Ora (Health New Zealand) to develop a micro-credential in cybersecurity. This will involve providing pathways for Maori and Pasifika students into entry-level cybersecurity roles to help fill skills gaps in the cybersecurity space, with Te Whatu Ora offering 10 paid cybersecurity apprenticeships under the partnership.[40]

> **“**
> **66% of New Zealand and Australian respondents cited that their cybersecurity teams are understaffed.**



India

As cyber threats continue to grow, India is seeing significant demand for cybersecurity professionals – globally, India ranks second when it comes to security threats on Cloud, surpassed only by the US.[41] However, most companies aren't equipped to deal with the magnitude of cyber threats that continue to come their way. A survey from global IT association ISACA reveals that 42% of Indian companies' cybersecurity teams are understaffed, and 60% of organisations have unfilled cybersecurity roles.[41]

Research also reveals that as of May 2023, there were 40,000 cybersecurity job postings in India[42], highlighting the pressing need for appropriately skilled talent. However, these candidates are in low supply and 59% of Indian companies feel that less than half of their cybersecurity candidates are appropriately qualified for the job they're applying for.[41] With a shortage of qualified applicants, Indian companies are finding it difficult to appropriately protect their data and systems.

The Government of India is attempting to fill the cyber skills gap through its program 'Future Skills Prime'. This is a joint initiative between the Ministry of Electronics & Information Technology (MeitY) and the National Association of Software and Services Companies (NASSCOM). The program is dedicated to upskilling and reskilling professionals in 10 emerging technologies, including AI, IoT and cybersecurity.[43] The Government also launched a Digital Skilling program in 2022 to offer skilling opportunities to students through apprenticeships, internships, and employment in the areas of emerging and future tech.[43]

> **59% of Indian companies feel that less than half of their cybersecurity candidates are appropriately qualified for the job they're applying for.**

United States

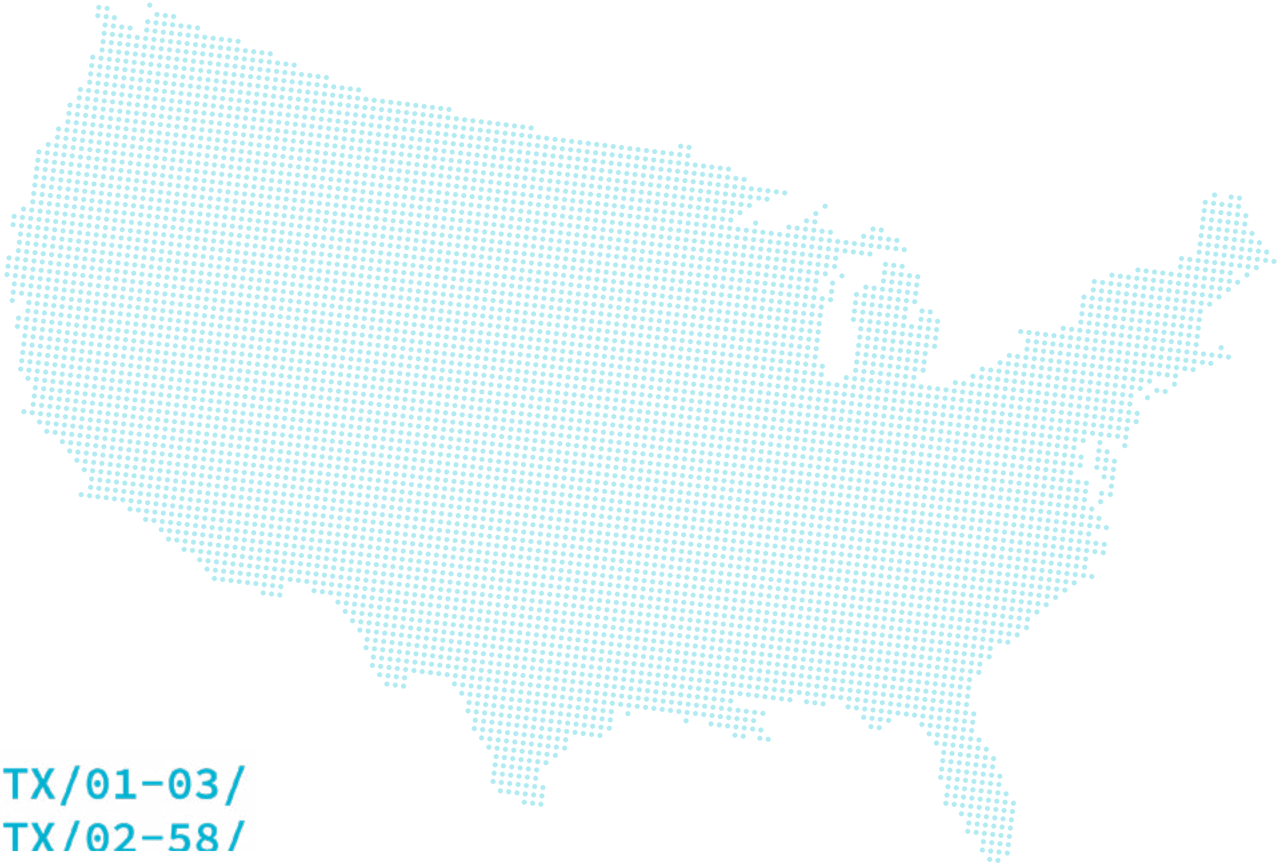
A 2022 survey of senior IT decision-makers in the US highlighted that 51% had experienced a cybersecurity breach over the past 12 months.[44] With more than 1 in 2 affected, cybersecurity is resultantly a top priority for companies across the US - 49% cited that improving threat detection was a top priority over the next year, followed by 48% citing a desire to improve threat response.

Making these goals a reality is only possible with the right people on board. However, the US is experiencing a cybersecurity worker shortage, with only 69 workers available for every 100 cyber jobs. This shortfall is placing strain on businesses as they attempt to secure their systems in light of growing cyber threats. In the past 12 months, there have been over 663,000 cybersecurity job postings across the country, however, with a shortfall of over 466,000 workers to fill these roles, candidates with the right skillsets are in significant demand.[45]

> **The US is experiencing a cybersecurity worker shortage, with only 69 workers available for every 100 cyber jobs.**

To meet this shortfall, investment has been made into cybersecurity training for students. In June 2023, Google announced an investment of over $20 million into establishing cybersecurity clinics at 20 higher education institutions in the US, offering students the chance to learn and upskill.[46]

The US government also invested $15.6 billion in cybersecurity for the 2023 financial year, with the bulk of the funding ($11.2 billion) directed into the Department of Defense (DoD), and $2.9 billion to the Cybersecurity and Infrastructure Security Agency (CISA). The funding for the DoD will be used to invest in the growth of 5 Cyber Mission Force teams to defend the country's national interests.[47]



The code to the cash: Cybersecurity salaries

With a global shortage of cybersecurity professionals, what does this mean for tech candidates with security skillsets? Demand is high, driving salaries even higher – globally at Talent, we have observed a 20% growth in security salaries in the past year[48], and we can only anticipate this will increase. Here is a snapshot of the latest cybersecurity salaries.

Salaries are for permanent roles and are noted per annum. They are quoted in local currencies and are exclusive of superannuation and 401(K). Contract rates are noted per hour. Please note, these are averages across each country and may not be reflective of your particular region. Salaries and contract rates vary per city due to factors such as location, industry, size of enterprise, hybrid/on-site work, etc.

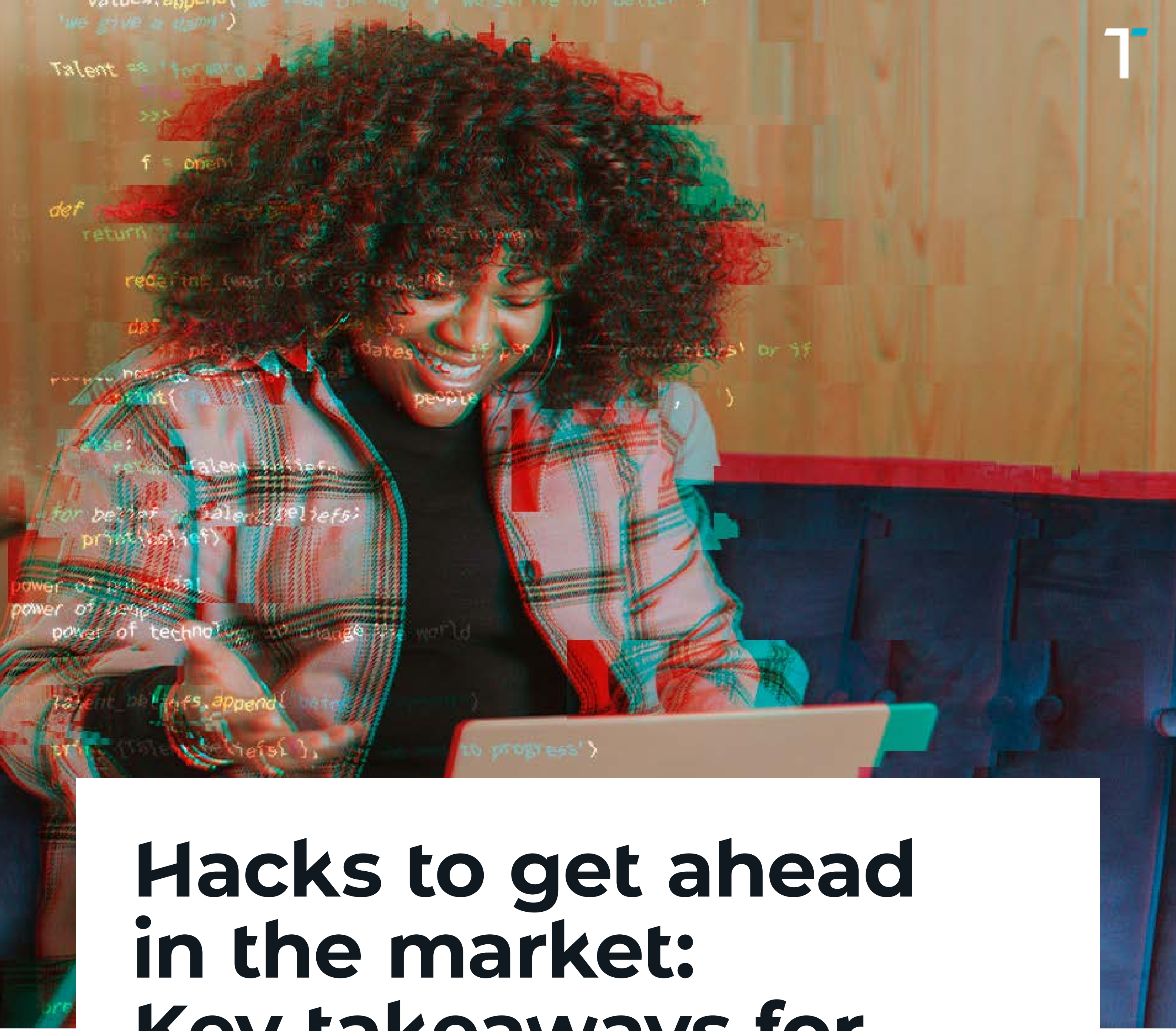
perm

Roles	AU avg.	NZ avg.	US avg.
Chief Information Security Officer (CISO)	$338k	$250k	$240k - $600k
Cloud Security Engineer	$168k	$158k	$140k - $210k
Cybersecurity Analyst	$133k	$105k	$102k - $145k
Cybersecurity Architect	$218k	$185k	$117k - $150k
Cybersecurity Consultant	$179k	$160k	$104k - $170k
DevSecOps Engineer	$175k	$158k	$138k - $175k
GRC Consultant	$143k	$140k	$128k - $200k
IDAM Consultant	$168k	$155k	$150k - $190k
IDAM Engineer / Developer	$148k	$135k	$130k - $160k
Incident Response Specialist	$170k	$130k	$125k - $175k
Penetration Tester (Ethical Hacker)	$173k	$115k	$130k - $190k
Security Operations Center (SOC) Manager	$204k	$135k	$122k - $160k
SIEM Engineer	$150k	$140k	$135k - $170k
SOC Analyst	$130k	$95k	$98k - $190k
Vulnerability Management Analyst	$138k	$120k	$125k - $175k

contract

Roles	AU avg.	NZ avg.	US avg.
Chief Information Security Officer (CISO)	$217	$215	$300 - $600
Cloud Security Engineer	$134	$148	$100 - $200+
Cybersecurity Analyst	$113	$95	$80 - $130
Cybersecurity Architect	$163	$145	$100 - $200+
Cybersecurity Consultant	$140	$148	$100 - $200+
DevSecOps Engineer	$141	$148	$80 - $140
GRC Consultant	$125	$115	$80 - $150+
IDAM Consultant	$128	$180	$80 - $120
IDAM Engineer / Developer	$117	$128	$80 - $120
Incident Response Specialist	$122	$115	$65 - $100
Penetration Tester (Ethical Hacker)	$124	$100	$50 - $90
Security Operations Center (SOC) Manager	$167	$135	$90 - $140
SIEM Engineer	$122	$130	$90 - $150
SOC Analyst	$90	$95	$80 - $150+
Vulnerability Management Analyst	$104	$105	$80 - $130

Uncover the average salary for your city in our More Than Money Salary Guide



Hacks to get ahead in the market: Key takeaways for candidates and employers

Whether you're a candidate who wants to get ahead in the jobs market and secure top cybersecurity opportunities, or a hiring manager who is seeking to attract top cybersecurity talent and keep them on board, here's everything you need to know.

If you're a candidate

Keep skilling up

Keep your skills up to date and you'll continue to be in demand. Cloud computing security, penetration testing, and security operations skillsets are what employers are seeking most. Plus, an open mindset and demonstration of continuous learning is a plus in the eyes of employers.

Get those certifications

When it comes to securing your dream role, employers are searching for candidates with the right qualifications. The most sought after? Certified Information Systems Security Professional (CISSP)[9]. It's an advanced certification, but if you're looking to take the next step in your career, this is the qualification you'll want in your arsenal.

Brush up on your communication skills

You could be amazing at what you do, but if you can't sell yourself and your work to key stakeholders, you could be putting yourself at a disadvantage. Communication skills are a key differentiator, and could mean the difference between you landing or missing out on your dream cybersecurity role. Honing your skills in this area will help you get a leg up in your career.

Stay informed

The industry is constantly changing and the threat landscape is evolving, so to get ahead in the jobs market, you'll want to remain aware of the latest happenings - think, the latest tech, regulations, threats and standards that are shaping this space. Consider signing up for cybersecurity newsletters, reading cybersecurity blogs and news outlets, and checking out the latest reports and whitepapers in this area. Joining LinkedIn groups and forums with other cybersecurity professionals is also a great way to keep your finger on the pulse.

If you're a hiring manager

Competition for top talent is tough, so you need to be putting your best foot forward if you want to get ahead. This is what top cybersecurity professionals are looking for:

A strong EVP

According to a LinkedIn Employer Value Propositions Survey 2022-2023, excellent compensation and benefits was cited as important to 68% of professionals skilled in cybersecurity, followed by flexible work arrangements at 52%, and organisational support to balance work and personal life at 47%.

A whole of business approach to cyber

No matter which sector you're in, it's not a matter of if an attack will happen, but when. To attract top cyber professionals, it's important that your leadership team and board recognise the risk and are willing to invest in and support cybersecurity infrastructure and initiatives. While they are talented, it takes much more than a new cyber expert to protect your organisation.

Purpose above all

For cybersecurity professionals, purpose is key. In our Talent Contractor Wellbeing Report, 86% of tech contractors emphasised the importance of connecting to their company's mission.[49] This desire expands to cybersecurity talent wanting to engage in meaningful work that contributes to the field's advancement.

Meaningful projects and career development

A 2023 Talent survey of over 500 tech candidates revealed that the opportunity for exciting and meaningful work mattered most to 85% of these professionals when looking for job. The opportunity for career progression and development was also a deciding factor for 48% when searching for a role. It's a great idea to ensure you're offering projects that challenge your people, and consider investing in training and development opportunities that will help them hone their skills and progress within your organisation. This will not only help you attract and retain top talent, but will also assist in strengthening your company's cyber defences.

Your sustain-ability

Sharing your sustainability efforts matters. Our Talent Sustainability: Awareness to Action insights report revealed that a noteworthy 84% of tech candidates want to work for a company that demonstrates a strong commitment to environmental sustainability. A significant 59% of these candidates consider a company's dedication to this cause as a determining factor when considering a job offer.[50]

Need help finding cyber talent or your next opportunity?

Keeping up and getting ahead of rapidly evolving cyber threats is tough. But don't worry, we've got your back. We work with a growing crew of cybersecurity experts (over 1,000) from all over the world, and a global network of clients spanning across all industries. Our team of recruitment specialists bring together experts in tech, transformation and beyond. So, if you're a top-tier encrypter and can spot malware in seconds, or an employer who is looking to build a high performing cyber team, we're here to help.

Ready to get started?

Reach out to Talent today

```
/TX.MZP: //
/PX.0WZ: //
{ref. xi2}
{ref. xi5}
```

Need help with a cybersecurity project?

We can support you with locking things down. At Avec, we offer specialised cybersecurity services, supporting leading-commercial companies through to government clients across Australia and New Zealand. Offering a full suite of strategic consulting, advisory, incident response, and managed security capabilities, we can help you strengthen your cybersecurity defences.

Ready to begin?

Reach out to Avec today

About Talent

Talent is a global technology and digital recruitment specialist committed to creating a better world of work for all. From simple beginnings in 1995, Talent now connects thousands of tech and digital professionals annually with a diverse range of organisations through its offices across Australia, NZ, and the US. The Talent group encompasses embedded recruitment service, Talent Solutions; specialised Microsoft recruitment service, Talent Microsoft; IT project delivery consultancy, Avec; youth employment charity foundation Talent RISE; and contractor experience platform ENGAGE. Talent brings real value to people and organisations by building highly skilled and engaged teams, rethinking technology solutions and improving lives by creating a strong sense of belonging.

for a better world of work

import brand_vision from Talent
values = brand_vision.values('values')
people == 'candidates'
people == 'colleagues':
('Talent cares about people)
power of technology to change the world
Talent_beliefs ('being different')
Talent_beliefs[ ], 'is the way to progress')
Talent is about people
Talent is about change

About Avec

Avec provides a value-driven alternative to traditional technology consulting, blending capacity and capability with our superpower—delivery. Our experienced consultants bring expertise, accountability, and an unwavering commitment to delivery to make life easier for our clients through Automation, Architecture, Business Analysis, Data, PMO, Testing and beyond. Together, we provide a refreshing, no nonsense, human approach to project delivery - empowering people and technology to build a better world of work, one project at a time.

Sources

1. https://dxc.com/au/en/insights/perspectives/article/five-cybersecurity-trends-that-will-shape-2023-and-beyond

2. https://www.infosecurity-magazine.com/news/global-cyber-attacks-rise-7-q1-2023/

3. https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

4. https://www.issa.org/cybersecurity-skills-crisis-continues-for-fifth-year-perpetuated-by-lack-of-business-investment/

5. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf?utm_source=pr&utm_campaign=report-2022-skills-gap-survey%5Ch

6. https://www.isaca.org/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-new-isaca-research-shows-retention-difficulties-in-years

7. https://www.hcamag.com/nz/specialisation/industrial-relations/how-government-and-industry-can-work-together-to-address-the-cyber-skills-shortage/418407

8. https://www.peoplematters.in/article/talent-management/cybersecurity-positions-in-india-remain-vacant-amid-dearth-of-qualified-talent-survey-33387

9. https://www.coursera.org/articles/popular-cybersecurity-certifications

10. https://www.equinix.com.au/newsroom/press-releases/2022/11/more-than-80-of-australian-businesses-are-reskilling-it-workers-in-response-to-the-growing-tech-skills-gap#:~:text=According%20to%20the%20Equinix%202022,main%20threats%20to%20their%20business.

11. https://www.techrepublic.com/article/aiia-survey-2023-australia-it-skills-shortage/

12. https://www.coresecurity.com/blog/how-manage-pen-testing-skills-shortage

13. https://www.statista.com/statistics/1291380/ai-in-cyber-security-market-size/

14. https://tech.co/news/businesses-have-cybersecurity-doubts

15. https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error#:~:text=Researchers%20from%20Stanford%20University%20and,caused%20by%20an%20employee%20mistake

16. https://blog.knowbe4.com/social-engineering-and-business-email-compromise-attacks-increased#:~:text=Awareness%20Training%20Blog-,New%20Report%20Shows%20Social%20Engineering%20and%20Business%20Email,Have%20Drastically%20Increased%20in%202023&text=Email%2Dbased%20social%20engineering%20attacks,to%20a%20report%20by%20Acronis.

17. https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware

18. https://www.linkedin.com/news/story/calls-to-sack-fake-phishing-victims-5775028/

19. https://cybersecurityventures.com/security-awareness-training-market-to-hit-10-billion-annually-by-2027/

20. https://venturebeat.com/security/report-cybersecurity-awareness-has-increased-to-97-in-last-year/#:~:text=Report%3A%20Cybersecurity%20awareness%20increased%20to%2097%25%20in%20the%20last%20year,-VB%20Staff&text=According%20to%20a%20new%20study,type%20of%20security%20awareness%20measures.

21. https://siccura.com/cyber-attacks-can-lead-to-employees-getting-fired-heres-how/

22. https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

23. https://purplesec.us/resources/cyber-security-statistics/#Education

24. https://news.sophos.com/en-us/2023/07/13/the-state-of-ransomware-in-financial-services-2023/#:~:text=The%202023%20survey%20revealed%20that,sector%20in%20the%202021%20report

25. https://www.americanbanker.com/news/cybersecurity-talent-shortage-in-banking-expected-to-grow#:~:text=Banks'%20struggle%20to%20hire%20cybersecurity,strategies%20since%20at%20least%202018.

26. https://www.ibm.com/downloads/cas/DB4GL8YM?_ga=2.176219234.652059713.1694753679-80142.1694753679&_gl=1*1bl62xo*_ga*ODAxNDIuMTY5NDc1MzY3OQ..*_ga_FYECCCS21D*MTY5NDc1MzY3OS4xLjAuMTY5NDc1Mzg2Mi4wLjAuMA

27. https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

28. https://www.databricks.com/blog/2023/03/01/cybersecurity-manufacturing.html

25. https://news.sophos.com/en-us/2022/09/07/the-state-of-ransomware-in-retail-2022/#:~:text=Retail%20reported%20a%2075%25%20increase,ransomware%20attacks%20across%20all%20sectors

26. https://www.retail-insight-network.com/news/retailers-are-failing-to-train-employees-in-cybersecurity/?cf-view

27. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/

28. https://www.himss.org/news/report-healthcare-cybersecurity-programs-face-workforce-shortage#:~:text=Healthcare%20cybersecurity%20professionals%20are%20a,organizations%20from%20hiring%20cybersecurity%20staff

29. https://www.cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022

30. https://www.washingtonpost.com/politics/2021/08/02/cybersecurity-202-governments-facing-severe-shortage-cyber-workers-when-it-needs-them-most/

31. https://practiceguides.chambers.com/practice-guides/cybersecurity-2023/australia/trends-and-developments

32. https://australiancybersecuritymagazine.com.au/75-of-australian-companies-overwhelmed-by-data-security/

33. https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3

34. https://securityintelligence.com/news/australian-government-invests-cybersecurity/

35. https://www.industry.gov.au/news/upskilling-and-diversifying-australias-cyber-security-workforce

36. https://www.cert.govt.nz/about/quarterly-report/quarter-two-cyber-security-insights-2023/

37. https://www.thelawyermag.com/nz/practice-areas/government/government-creates-lead-operational-agency-to-strengthen-cyber-security/454702

38. https://www.defence.govt.nz/what-we-do/delivering-defence-capability/defence-capability-projects/cyber-security-and-support-capability/

39. https://www.oecd.org/employment/building-a-skilled-cyber-security-workforce-in-five-countries-5fd44e6c-en.htm

40. https://www.nzherald.co.nz/kahu/social-enterprise-focussed-on-growing-maori-and-pacific-leaders-as-cyber-security-experts/VTS5F2RQT5GMZFKGX5OD5W3IF4/

41. https://www.peoplematters.in/article/talent-management/cybersecurity-positions-in-india-remain-vacant-amid-dearth-of-qualified-talent-survey-33387

42. https://cybermagazine.com/cyber-security/india-witnesses-demand-for-40-000-cybersecurity-jobs

43. https://www.investindia.gov.in/team-india-blogs/need-securing-ai-blockchain-and-cybersecurity-talent

44. https://nz.insight.com/content/dam/insight-web/en_US/pdfs/insight/the-path-to-digital-transformation--where-leaders-stand-in-2023.pdf

45. https://www.prnewswire.com/news-releases/shortfall-of-skilled-cybersecurity-workers-in-the-us-reaches-an-estimated-466-000--cyberseek-data-reveals-301843552.html

46. https://blog.google/inside-google/message-ceo/commitment-cybersecurity-workforce/

47. https://securityintelligence.com/articles/how-much-is-us-investing-in-cyber/

48. https://www.betterworldofwork.io/more-than-money/salary-trends

49. https://www.talentinternational.com/contractor-wellbeing-report-21-22/

50. https://www.betterworldofwork.io/sustainability-intro