How to pursue a career in cybersecurity

Career
with ACS

Introduction

The prevalence and sophistication of cyber threats have heightened the need for highly skilled cybersecurity professionals. Cybersecurity is critical to all businesses today, and the variety of cyber roles and responsibilities is unrecognisable from a few years ago. Consequently, cybersecurity is an exciting career choice for a diverse cohort, utilising different technical and interpersonal skills and accommodating many motives whether you want to make a difference in society, focus on niche skills or simply enjoy job prospects and security, there's a cybersecurity career for you.

The other good news? There are oodles of formal and non-formal pathways into a cybersecurity career. While many in the workforce have completed an ICT or cybersecurity degree, others kicked off their journeys with microcredentials, choosing a free or paid entry-level industry certification to start building cybersecurity nous. Several found internships within organisations or the public sector, giving them the opportunity to try some of the huge array of cybersecurity tasks out there today before finding their specialty. Others found mentors or attended events and networked with the cybersecurity community, more great ways to navigate into this vibrant, fast-growing and important profession.

The not-so-good news? One linear pathway to becoming a cybersecurity professional in Australia doesn't exist. With so much opportunity comes diversity, and cybersecurity can feel a spaghetti junction of a space at times. Numerous employers will tell you, for example, it's advantageous to have technical knowledge, especially around networking and programming languages. Completing a dedicated cybersecurity or blended IT/cybersecurity degree at university is arguably the best way to get a leg up generally, and specifically if you want to become a threat hunter, vulnerability tester or security architect.

Yet in other cases where you're educating others on how to proactively mitigate cyberattacks, business and management experience along with great communication skills sharpened in another sector can prove very useful. And if you're a school student who simply loves trying to hack systems to see how they work, such inquisitiveness also holds you in good stead.

What's more, while formal tertiary and industry certifications can fast-track your cybersecurity career, there's nuance in what employers seek across different industries, particularly in a governance versus technically oriented role. What the majority agree, however, is a passion and curiosity for what you COULD achieve as a cybersecurity professional is a must.

This ACS Careers Guide in Cybersecurity is not designed to tell you the one way to become a cybersecurity professional – there simply isn't one. What we aspire to do is provide insight into common requirements, certifications, occupations and ways of engaging in the industry that improve your chances of steering towards the right cybersecurity role for you – with some markers depending whether you're a school leaver, uni graduate, IT specialist looking to upskill, or other professional looking to reskill. We've talked to cybersecurity professionals to unveil what it really means to be in this dynamic ecosystem, and their advice on getting a foothold.

We've talked to cybersecurity professionals to unveil what it really means to be in this dynamic ecosystem, and their advice on getting a foothold.

Why you should consider a career in cybersecurity

Cybersecurity is one of the most in-demand disciplines globally, and as business and society continue to integrate internet-connected technology into every part of our lives, it's a sector where demand – and roles pertaining to managing and tackling cybersecurity – are only going to increase.

According to the Australian Cybersecurity Centre (ACSC), over 94,000 cybercrimes were reported for the 2022-2023 financial year alone. That's over 250 attacks a day, every day – an average of one every six minutes. The cost of these incidents just keeps increasing, up 14% in the past year. And that's only the ones we know about.

But more than that, cybersecurity is about stitching together technical, digital and information security risks to broader business risks. That's because cybersecurity is a risk for any organisation, large or small, and all must navigate and mitigate exposure to get on and do business.

Recognising the importance of cybersecurity as both a national security and economic imperative, recent Government initiatives to support the sector include:

- **Australian Cybersecurity Strategy:** A $587 million, seven-year plan to boost Australia's cybersecurity capability by 2030, including $129.7m for building regional cybersecurity resilience and $290.8m to protect business and citizens from cyber attacks.

Top five sectors for cybersecurity roles

1. Professional, scientific or technical services
2. Public administration and safety
3. Healthcare and social assistance
4. Financial and insurance services
5. Education and training

- **Australian Defence Force Cyber Gap Program:** $41m allocated to financially support and mentor cybersecurity students, as well as provide them with defence work experience opportunities.
- **The Cybersecurity Skills Partnership Innovation Round:** The second round of this program, worth $60m, is providing funding of up to $3m to fund 50% of eligible project expenditure for organisations looking to find new ways to improve the quality and availability of cybersecurity professionals in Australia.
- **The Cybersecurity Work Integrated Learning pilot:** Sitting within the Canberra Cyber Hub, this co-design, public/private sector initiative is designed to bridge the gap between tertiary education and the skills employers need in the workplace. It does this by offering free access to facilities, trainers, a 4-week bootcamp and four micro-credentials for cyber analysts.

A career in cybersecurity is not only in high demand, it can make a tangible difference to Australia's economy and sovereignty. Without cybersecurity, we wouldn't be able to rely on the infrastructure, products and services we all depend on every day. Cybersecurity is critical and fundamental to the success of the nation as a whole.

Five most requested skills for cybersecurity roles

1. Information security
2. Network security
3. ISO 27001
4. Linux
5. Cisco

Australia's Federal and state governments are primary employers of cybersecurity professionals. After public sector, the biggest employers are management consulting and public accounting firms. The highest concentration of job openings focuses on securely provisioning IT systems, followed by operating and maintaining IT system performance and security, then overseeing and governing an organisation's cybersecurity framework.

Snapshot of the cybersecurity jobs market

$99,000
Average wage for cybersecurity specialist in 2023

16.2%
Average wage increase for cybersecurity professionals 2019-2022

16%
Entry-level (0-2 years' experience) jobs in cybersecurity

79%
Cybersecurity workers with jobs in the private sector

$111,584
Average advertised salary for cybersecurity roles in 2023

13,160
Dedicated and related cybersecurity job openings in Australia in 2023

101%
Growth in jobs over the past 5 years

21%
Jobs in the public sector

Source: AustCyber Explorer 2022 + 2023

What does a cybersecurity specialist do?

At a technical level, cybersecurity runs the gamut of ICT applications, from software and development to data and networking, identity and access. Security isn't just one facet of any given platform, it's a systemic practice from top to bottom. It spans every piece of hardware, software and policy, digital and physical system, and all people that exist throughout any given ICT ecosystem, end-to-end.

Security threats can come from almost as many sources – state actors, terrorism, crime, identity theft, ransomware, spyware and many more. There are as many reasons to protect a system as there are reasons to enter it. As a result, cybersecurity isn't a single career path. It covers a breadth of education, skills and specialisms, each with their own domains focusing on one or more facets of the overall security landscape.

ICT in general moves at a fast pace, changing regularly and always introducing something new. This is even more the case for cybersecurity. To keep systems, data, infrastructure and access secure, you can be involved in a real-time arms race, rapidly responding to changes in how attacks occur.

Key disciplines of cybersecurity both in dedicated roles as well as within broader ICT roles include:

- ✓ risk management
- ✓ security architecture and engineering
- ✓ communications and network security
- ✓ identity and access management
- ✓ security assessment and testing
- ✓ security operations
- ✓ asset security management
- ✓ secure practices used in coding and development
- ✓ governance and compliance.

Day-to-day and depending on specialisations, a cybersecurity position involves planning, evaluating and implementing security to protect systems and networks; monitoring and reporting on vulnerabilities and breaches; simulating attacks to test defences; keeping software and operating systems up to date with security patches; staying abreast of latest developments in the field; and educating staff and key stakeholders on security best practice. Just as in other areas of ICT, each of these can be a full-time role, depending on organisation.

Then there's the lateral thinking the majority of employees are looking for. While there may be necessary playbooks and crisis management protocols for tackling a cybersecurity incident, being able to apply a different lens or way of thinking to a situation can be extraordinarily useful if you're a cyber defence incident responder, intrusion detection specialist or a red team leader tasked with looking at problems and situations from the perspective of an adversary.

Other domains of focus

Cybersecurity isn't just a technical profession either. Increasingly, the context an organisation operates in, the growing imperative to prepare and mitigate cyber threats and attacks, the rise in digital information sharing and storage, and the commercial, reputational, customer harm and employee ramifications of an incident or data breach, have seen cybersecurity specifically, and information security more broadly, become crucial to doing business today.

Most government contracts, for example, expect providers of ICT services to prove they provide regular security awareness programs. Given the convergence of Privacy, Assurance and Physical Security with cybersecurity, security awareness is becoming more important to every organisation, from board and executive level through to line-of-business users.

In turn, there's an ever-expanding roll-call of business-oriented roles within the cybersecurity profession and wider ecosystem. While these positions benefit from having technical knowledge and experience across the tools, platforms, programming languages and IT systems and software listed in this guide, what's equally critical is having business knowledge, communication and interpersonal skills, and a willingness to keep up with regulatory and privacy legislation and obligations across territories.

This is where Governance, risk and compliance (GRC) comes into play.

GRC is a centralised organisational strategy for managing governance (such as policies and rules), risk management (such as assessments and frameworks) and compliance (regulatory, legislative and legal) with industry and government regulations. GRC's set of practices and processes help companies effectively manage IT and security risks, reduce waste, increase efficiencies, reduce non-compliance risk, and share information more effectively.

GRC for security enables organisations to employ data security measures to protect customer data and private information. It also helps an organisation comply with data privacy regulations like the General Data Protection Regulation (GDPR) in Europe, and the Security of Critical Infrastructure Act in Australia, avoiding commercial losses, fines and penalties.

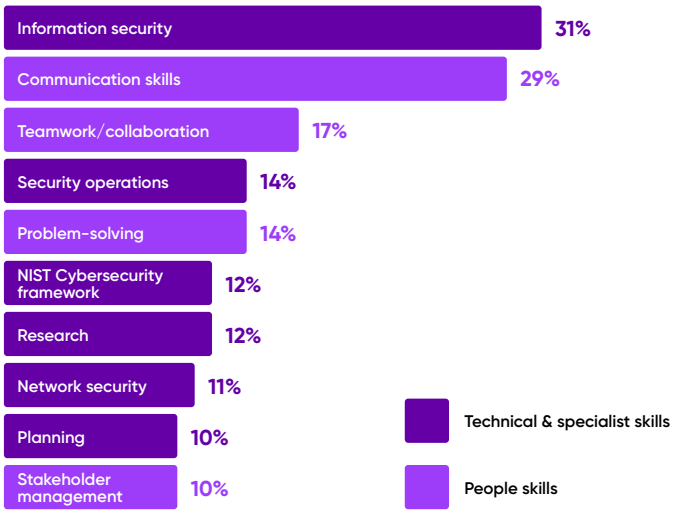
As well as strategy, GRC can refer to an integrated suite of software capabilities for implementing and managing an enterprise GRC program. We've highlighted three examples of GRC roles, but there are plenty more.

Auditor: Independently reviews and evaluates systems' configurations, records activities to determine the adequacy of system controls, ensures adherence with established security policy and procedures plus compliance with laws and regulations, identifies control failures or gaps, detects breaches in security services, and recommends changes specified for countermeasures and continual improvement.

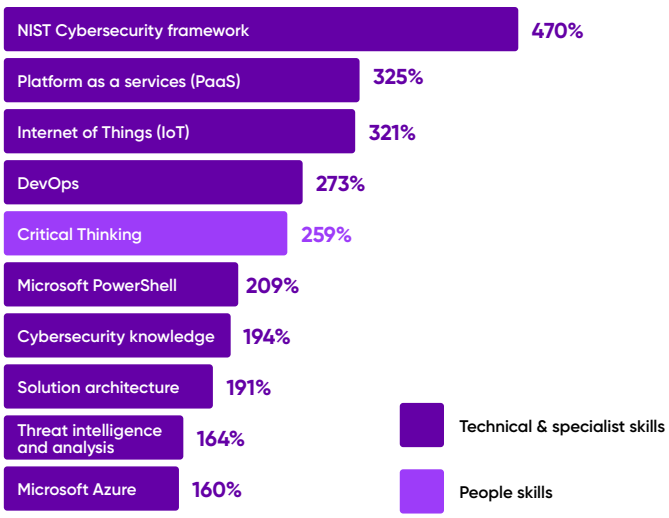
Risk Analyst: Undertaking an advisor role in between audit and the operation, the security Risk Analyst conducts inventories and assessments, identifying and analysing the risks in the organisation, the technology, the data, and processes. This role verifies controls are in place and operating as expected to protect against security threats.

Data Governance: Working at the intersection of customer engagement, data lifecycle management and privacy and data architecture, specialists in this area will collaborate and advise colleagues and ICT practitioners ensuring that privacy programs, laws, and practices are followed during the design, development, and implementation of systems, applications and infrastructure. They may also draft policies or conduct privacy impact assessments (PIA) and other privacy-focused assessments.

Top 10 occupational skills



Top 10 skills with growing demand



Day in the life of a cybersecurity professional

Confronting the adversary

Meet Ashwin

Name: Ashwin Pal

Current job: Partner, Cybersecurity, RSM Australia

Years in cybersecurity: 25

Formal training and education: IT degree, CISSP, CISA, ISACA and ISC2 certifications.

I'm a cybersecurity professional because... Cyber is so much more than IT; it's pervasive in everyone's lives, as much as information technology today. And it's gaining more complexity. Attacks are going to continue. At the moment, the disincentives – the controls, catching people and the penalties – are much less than the incentives. That sums up what cybersecurity is: It's cops and robbers, cat and mouse. You choose which side you're on. The skills are very similar regardless of which side you're on, and there's a thin line that separates good from bad.

The biggest challenge I've experienced... is the sophistication and complexity of the adversary. When you come up against nation state attackers, you really are locking horns with a worthy adversary.

One unique thing I do every week... is I advise clients and businesses on what cyber risk is; help them be able to understand it properly; then have conversations about how you mitigate and manage risk.

It's impossible to eliminate the risk. What you do is take all necessary measures and put in controls to make sure you don't fall victim. I'm as much a businessperson as I am a cyber person. I'm advising boards and risk committees every day. Someone who remains technically specialised may go down a very different path.

> Within 12 months, my practice was recognised as the largest cybersecurity business in the country.

A career highlight... back in New Zealand was when I was shoulder tapped to join the largest systems integrator, Gen-I, part of Telecom NZ (now Spark Digital) to start up the cybersecurity business at the age of 25. It was super exiting, challenging and scary. Within 12 months, my practice was recognised as the largest cybersecurity business in the country.

Top tips:

For school or uni leavers:

You don't have to, but it does help to get a formal qualification in cyber. It will help you understand the ins and outs, so you don't get a shock when you start a job. If you don't, you'll get into it, but you may have a slower uptick of 1-2 years to get on a level playing field with someone who does. But cyber is still in a space where you can be trained on the job; I learnt everything I know on the job.

For upskillers or reskillers:

What you see a lot of in cybersecurity is ex-armed or police force professionals. That's because the training they have, plus investigative mindsets and attitudes, make them great cybersecurity professionals. When we're doing cybersecurity reviews, it's about asking the 'why' until you get to the answer. Either that reveals a company is doing the right thing, or there is a gap to fill and you need to make a recommendation before it gets exploited.

Timeline

- Completes an IT degree with information systems management major, qualifying as a business analyst
- Completes a number of industry certifications – CISSP, CISA – prioritising ISACA and ISC2 certifications
- Moves with Gen-I to Australia to establish and grow the Security / Information Risk Management practice
- Joins RSM as Partner for Cybersecurity and Privacy solutions for Australia
- Becomes first non-accounting, IT graduate hired by PwC in Wellington, NZ for a new cyber practice being set up
- Appointed as lead for Computerland NZ's first cybersecurity practice/ principal consultant
- Becomes Director of Cybersecurity APAC for Unisys

Is cybersecurity right for me?

The incredible breadth of role and remit cybersecurity professionals hold is staggering, making it a huge area of opportunity for school leavers, university graduates, existing IT professional and those looking to shift out of other categories.

For example, investigative skills are hugely important in most cybersecurity tasks, making those who come from armed forces or police a good pool of candidates for a switch in cybersecurity.

Nurses come into cybersecurity because they're very cool and calm when it comes to crises.

Equally, the need to translate complex, technical or risk issues arising from cybersecurity to non-technical employees across an organisation means strong communications and narrative skills are vital. People skills enabling you to build strong relationships across departments and all kinds of staff are equally critical in more business-oriented, advisory cybersecurity positions.

If you're already in the workforce, another valuable input is what industry you're transitioning from. "In GRC, we have women who came from the travel industry who understand businesses processes and risks well because they had that in travel," Australian Women in Security Network Founder and Executive Director, Jacqui Loustart says. "They can therefore ask those same questions when it comes to the cybersecurity part. Or nurses come into cybersecurity because they're very cool and calm when it comes to crises; they can triage and are very smart, they want to help people – so the protecting part is inertly where a lot of women come from."

In 2021, the education qualifications of cybersecurity professionals was split as follows:

- **44%** Undergraduate
- **25%** Postgraduate
- **15.5%** Vocational
- **11.5%** No post-school qualification
- **4%** Graduate

According to workplace performance experts, Hogan, the eight key personality traits for cybersecurity professionals are: Modest, altruistic, composed, scientific, inquisitive, sceptical, responsive and diligent.

Interpersonal skills

While ICT roles often have a degree of change, security takes that 'change and ambiguity' to a whole new level. Often, a cybersecurity professional must be comfortable with interrupting unfinished tasks and functions and immediately switch tasks to accomplish 'just-in-time' work. Additionally, one must be comfortable both asking hard questions of peers and informing leaders and executives of potentially 'bad' news.

Then there's the need to be able to influence cross-functional colleagues and teams of the criticality of performing certain tasks, upgrades or training in order to prevent and mitigate cybersecurity and wider information security incidents.

All this means cybersecurity professionals often benefit from certain personality traits as well as people-oriented skills in concert with technical, process and specialist skills required in specific roles.

An ACS Canberra Hub taskforce has looked to rate the attitudes, aptitude and work experience required for various cyber professions. In 2023, the taskforce came up with six key attributes across entry, mid and senior-level roles: Problem solving, organisation, initiative, technical, management and behavioural.

For instance, specific cybersecurity technical skills are more important when you're in a hands-on, entry-level role or with limited domain exposure. So are general IT skills. As you move up the ladder, people skills become even more critical, as are project management skills.

Fast facts

67%

Male cybersecurity professionals have education qualifications in IT.

50%

Female cybersecurity professionals have IT qualifications. A large portion come into the sector with qualifications in business and management, humanities and creative arts.

Day in the life of a cybersecurity professional

Thirst for knowledge

Meet Stephen

Name: Stephen Bennett

Current job: Group Chief Information Security Officer, Domino's

Years in cybersecurity: 25 years

Formal training and education: Polytechnic in England studying IT; Cisco, Microsoft vendor qualifications; OSCP (Offensive Security Certified Professional).

I got into cybersecurity because… I had the right mindset: Thirst for knowledge, eagerness to learn. I'd hack around on computers/electronics to try and fix an issue, make life easier, or for entertainment. In the UK, I dealt with supplying and installing retail systems and discovered a major configuration vulnerability that meant you could control ISP routers. That was a lightbulb moment where I thought 'hey that's really cool, how I could do more of that?'. When I moved to Australia, I shifted to dedicated cyber roles.

A surprising part of the job… is its breadth and depth. It's impossible to know everything in cyber. I had to 'let go' and rely on teammates to take up the slack. But that's a huge plus side of this profession: It's so vast.

The biggest challenge I've experienced… is recognising cybersecurity is not you versus the world; you have to talk to people more than you realise, cross functionally, to get them to prioritise the stuff you need them to do for the benefit of the organisation. I'm introverted and struggle with this aspect.

The reason I love being a cybersecurity professional… is the same reason it's challenging: It'll never stop evolving. When I tell people I work in cyber and what I do, especially as it's just so prevalent in the media, that's a great feeling. Even better than that is providing guidance to friends and family to prevent them from being cyber victims. As a cybersecurity team, there's a lot of camaraderie, which is another big benefit.

> When I tell people I work in cyber and what I do, especially as it's just so prevalent in the media, that's a great feeling.

One unique thing I do every week… is choose a 'victim' from the team who presents security news to their colleagues. I also check-in and see how we're doing with support calls to work out what can we automate, what we can't. Every month, I sit down and do support calls for half a day.

Top tips:

For school or uni leavers:

Be passionate. I'll quiz people and ask: Are you interested in security? What do you do to cultivate this interest?

For upskillers or reskillers:

Talk to people in the industry, attend local security events. Security people are very welcoming. Try and find a mentor, or friend of a friend – or even a complete stranger. If you're really interested, it goes back to the passion and persistence. And recognise the position you start in isn't necessarily what you're going to be doing long term. Another tip is cyber isn't just for people in hoodies sitting in their room coding in the dead of night. There's so much more to it.

Timeline

- Completes a Diploma in Computer Science at UK polytechnic (VET)
- Becomes IT trainer / assessor for several organisations
- Becomes IT manager for various government and private sector firms
- Gets security / communications engineer position, marking first step towards cybersecurity role
- Relocates to Australia and joins Queensland Police as IT Security Leader
- Gains OSCP (Offensive Security Certified Professional) accreditation on top of other vendor networking certs
- Joins Domino's as group security manager and gains c-suite exec role

Key questions to ask yourself

A few questions worth posing as you look to explore which pathway is best for you in the cybersecurity field are:

What are my personal passion points?

Is it getting down and dirty and understanding robotics? Is it data analytics? Is it talking to people? Is it selling? It is hacking code at midnight? Finding out your passion points can help indicate the pathway in the cybersecurity ecosystem where you may be a good fit.

Do I enjoy getting analytical or am I a blue-sky thinker?

Do I like delving into the weeds to figure something out? Or am I drawn to the bigger picture, and thrilled by the prospect of strategising and building out the big picture view of an opportunity?

Am I a cool head and calm operator?

What am I like in a fast-moving situation or when faced with a problem? Am I perceived as a calm influence over others? Cybersecurity professionals are usually resilient, with penetration testers and those involved in rapid-fire incident response to a cybersecurity situation able to manage stress better than others.

Are my communication skills strong?

How good am I at articulating a problem and possible solution to others who don't have the same knowledge or insights as me? Do I understand technical concepts easily and can then translate into what that means for a business in terms of risk?

What am I curious about?

What is it about cybersecurity that's perked my interest? Why am I curious about pursuing a career in cybersecurity? What motivates me to learn?

Am I a problem solver?

Am I someone who likes to get to the bottom of a problem and will stick at it until I do? How do I rate my level of critical thinking?

Fast facts

An Australian Information Security Association survey of 650+ cybersecurity professionals found the strongest influences for why people look to commence a career in cybersecurity are:

- They're motivated to make a difference in society
- They enjoyed the fields of study that relate to the security industry
- The sector offers an opportunity to use their skills
- The considered job security and employment prospects in the industry
- The industry offers opportunities suited to their work preferences

Cybersecurity professionals are usually resilient, with penetration testers and those involved in the rapid—fire incident response to a cybersecurity situation can work under stress better than others.

Checklist of critical people skills most in demand in cybersecurity

- ✓ analytical problem-solving
- ✓ attention to detail
- ✓ lateral thinking
- ✓ communication skills
- ✓ organisational skills
- ✓ stakeholder management
- ✓ curiosity with a desire and willingness to learn

Employer insights

What your next boss is looking for

Just what is it employers are looking for when they go to hire new cybersecurity professionals to their teams? Are there pathways they prefer when hiring? And are there key attributes they're keen to see exhibited?

"When I hire staff, what I look for besides technical skills – although a lack of skill is not necessarily a problem – is aptitude. It's about critical and lateral thinking. Attention to detail is also extremely important. When you're looking at a problem, or investigating a security incident, you may not encounter a textbook situation or response. While we might have what we term playbooks, that's not always going to apply, because so many nuances are involved. Being contextually aware is extremely important in those situations. When we have a data breach, the definition of serious harm to an individual requires us as professionals to put our critical thinking hats on. We need contextual awareness to understand or interpret whether a potential breach is actually going to cause serious harm."

Jerome Chiew
Director, Critical IT and ACS WA Chair

"It has to be a combination of study, certification, experience and cultural fit within the organisation and within the security team. Written and good communication skills are exceptionally important too. You need to be able to learn quickly and on the move in security as nothing remains the same for very long."

Jo Stewart-Rattray
Director of Technology and Security Assurance, BRM Advisory

"InfoSec people should be spending time with businesses helping to design resilient processes before things go wrong. To achieve this, we need to attract diversity of thought, so business studies students should be encouraged."

John Baird
Founder and CEO, Revio Cyber Security

"A common misconception about cybersecurity is it's only for highly technical people who have hacked systems and codes to build better, more robust systems. That is not always the case. A cybersecurity professional is, at their core, an analytical person who looks at a problem from multiple points of view and devises an approach to solve the problem. When doing so, they must collaborate with people from different backgrounds and functions to understand the problem in-depth and in context. This requires good communication skills, unlike some other technology-heavy roles in which a specification is provided and the task is strictly to achieve it."

Deepa Seshadri
Partner, Deloitte India, for ISACA

"The most important educational capabilities for a successful career in cybersecurity are curiosity, tenacity, creativity, critical thinking, and leaning towards contrarian thinking."

Joe Dalessandro
Founder and CEO, Sirius Matters

"Sometimes you might face an issue where following the book won't solve it. If you can think well, actually, have you thought of doing it this way, that really works. That's where getting people from different backgrounds is helpful. I recruited an intern who had just completed a degree in criminology, and who had found the cyber content particularly interesting. She joined us one day a week to get an idea of what it was like to work in cyber and ended up staying on. This person definitely wasn't technical, but we found she was really good with images and the graphic design side of things and was also very organised. That intern is now heading up our awareness training across the whole group."

Stephen Bennett
CISO, Domino's

Guide to eight common cyber occupations

Top 10 cybersecurity jobs in Australia

1. Cybersecurity Analyst
2. Business Intelligence Analyst
3. Security Engineer
4. Senior Network Engineer
5. Cybersecurity Engineer
6. Network Engineer
7. Security Architect
8. Security Analyst
9. Intelligence Analyst
10. Cybersecurity Specialist

Because cybersecurity is such a wide field, and organisations have their own requirements within the realm of security, you'll find certain specialisms come under a banner of similar titles – for example, the roles of 'Cybersecurity Engineer' and 'Information Security Engineer' are likely to list the same key requirements for education, skills and experience.

There's also the associated 'information security' field. These two terms can be used synonymously, and there is debate among experts regarding how much disciplines overlap. However, most agree on a few distinctions. As the University of Adelaide puts it, cybersecurity has traditionally had an overarching mission of protecting computers, networks, information, and devices from malicious activity within cyberspace. This makes risk management the central focus, with an aim to increase an organisation's defences against various types of cyber-attacks. Cybersecurity professionals need to identify and protect all technological assets, understand an organisation's risk profile, and create and implement incident response plans, while ensuring legal and regulatory compliance.

On the other hand, information security is primarily concerned with securing data confidentiality, integrity, and availability and is gaining importance in an incredibly data-driven world. Information security is a crucial part of any cybersecurity strategy. Information security professionals perform a more specialised role overseeing access to information for organisations internally and externally, ensuring compliance with data security regulations and safeguarding access to data in the event of an attack.

As a result, there are more general, foundational cyber certifications you will come across, then others that are role specific or covering a specific area of cybersecurity – operations versus asset security or software development, for example.

Our advice is to research what the typical role requires as well as what the day-to-day tasks might be to ascertain your affinities and level of interest. Don't think of this as a one-way or linear path to ever-narrower job descriptions however: Given how often skills and knowledge requirements are shared between different specialisms, there are many ways to switch up your career.

Don't think of this as a one-way or linear path to ever-narrower job descriptions.

In the following pages, we highlight eight common cybersecurity roles covering at least one of the key disciplines mentioned earlier.

If you're not sure quite what type of role you want to go for, first look at the key disciplines that interest you, then the type of specialisms these may involve.

These occupations have been graded against the SFIA global skills and competency framework, which encompasses seven levels of responsibility:

1. Follow

Performs routine tasks under supervision, follows instructions and requires guidance to complete work.

2. Assist

Provides assistance to others, works under general supervision, uses their discretion to address routine problems.

3. Apply

Performs varied tasks, sometimes complex and non-routine, using methodical approaches. Works under general supervision, exercises discretion, manages own work within deadlines.

4. Enable

Performs diverse complex activities, supports and supervises others, works autonomously under general direction, contributes expertise to deliver team objectives.

5. Ensure/advise

Provides expert guidance in their specialty and works under broad direction. Accountable for achieving workgroup objectives and managing work from analysis to execution and evaluation.

6. Initiate/influence

Has significant organisational influence, makes high-level decisions, shapes policies, demonstrates leadership, and accepts accountability in key areas.

7. Strategy/inspire/mobilise

Operates at the highest organisational level, determines overall policy and strategy, assumes accountability for overall success.

Eight common cybersecurity occupations

Cybersecurity Analyst

Focus of role

Analyses and assesses vulnerabilities in the infrastructure, investigates available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices. Analyses and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions.

Titles of roles

ICT Security Analyst, Information Security Analyst, Cybersecurity Researcher, Vulnerability Researcher, Cybersecurity Vulnerability Assessor, Cyber Threat Analyst, Malware Analyst

Level of responsibility

(SFIA 1-7) 2,3,4,5

SFIA key five skills for this role

Information management (IRMG), Information security (SCTY), Security operations (SCAD), Threat intelligence (THIN), Vulnerability research (VURE)

Tools and platforms commonly used

- **Packet sniffing:** These tools sample the packets that travel over a network, analysing them and logging data. This can help a cybersecurity specialist better understand the data traversing a network. Tools for packet sniffing include tcpdump, Wireshark and WinDump.
- **Network and systems security monitoring:** Tools used to analyse the status of a network and look for network-centric threats include Nmap, Nagios, Splunk, Argus and OSSEC.
- **Encryption tools:** Encrypting data prevents it being accessed or readable by unauthorised users. Popular tools include TrueCrypt, VeraCrypt and KeePass.

Technical / IT systems proficiency

(Options: high, medium or low):

Medium

Programming language proficiency

(Options: mandatory, preferred, not required):

Preferred

Typical qualifications

Bachelor's Degree, Secondary School Education, practical work experience and training

Relevant certifications

Beginner / intermediate

CompTIA Security+ – Industry certification, covers asset security, security and risk management, security assessment and testing, software security, security operations.

Cisco Certified Network Associate (CCNA) Security – Vendor certification, covers communication and network security.

Advanced

CompTIA Cybersecurity Analyst (CySA+) – Industry certification for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring.

GIAC Security Leadership (GSLC) – Industry certification, validates a practitioner's understanding of governance and technical controls focused on protecting, detecting, and responding to security issues. GSLC certification holders have demonstrated knowledge of data, network, host, application, and user controls along with key management topics that address the overall security lifecycle.

Expert

CompTIA Advanced Security Practitioner (CASP+) – Advanced industry certification for security architects and senior security engineers covering technical skills in on-premise, cloud native and hybrid environments, governance, risk, and compliance skills, assessing an enterprise's cybersecurity readiness, and leading technical teams to implement enterprise-wide cybersecurity solutions.

ISC2 Certified Information Systems Security Professional (CISSP) – Industry certification, covers network security, identity and access management, security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, and security operations.

Eight common cybersecurity occupations

Cybersecurity Assessment and Advice Specialist

Focus of role

Conducts risk and security control assessments, interprets security policy and contributes to the development of standards and guidelines. This role reviews information system designs, provides guidance on security strategies to manage identified risks, provides specialist advice , explains systems security and the strengths and weaknesses.

Titles of roles

Cybersecurity Adviser, Cybersecurity Consultant, ICT Security Adviser, ICT Security Consultant

Level of responsibility

(SFIA 1-7): 3,4,5,6

SFIA key five skills for this role

Information security (SCTY), Risk management (BURM), Specialist advice (TECH), Threat intelligence (THIN), Vulnerability research (VURE)

Tools and platforms commonly used

- **Packet sniffing:** These tools sample the packets that travel over a network, analysing them and logging data. This can help a cybersecurity specialist better understand the data traversing a network. Tools for packet sniffing include tcpdump, Wireshark and WinDump.
- **Network and systems security monitoring:** Tools used to analyse the status of a network and look for network-centric threats include Nmap, Nagios, Splunk, Argus and OSSEC.
- **Vulnerability assessment and scanning tools:** These are designed to look for known vulnerabilities that a malicious actor could use to gain entry to a system or network, such an organisation's public-facing websites. Examples include SQLMap, Nikto, Paros Proxy and Burp Suite.

Technical / IT systems proficiency

(Options: high, medium or low):

Medium

Programming language proficiency

(Options: mandatory, preferred, not required):

Not required

Typical qualifications

Bachelor's Degree, Secondary School Education, practical work experience and training

Relevant certifications

Beginner / intermediate

CompTIA Security+ – Industry certification, covers asset security, security and risk management, security assessment and testing, software security, security operations.

GIAC Security Essentials Certification (GSEC) – Industry certification, covers security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations.

Advanced

ISACA Certified Information Systems Auditor (CISA) – Industry certification, covers security and risk management, security assessment and testing.

GIAC Security Leadership (GSLC) – Industry certification, validates understanding of governance and technical controls for protecting, detecting, and responding to security issues. Demonstrates knowledge of data, network, host, application and user controls along with security lifecycle.

ISACA Certified in Risk and Information Systems Control (CRISC) – Industry certification for business resilience and risk management. Covers IT governance, risk assessment, response and reporting.

Expert

ISACA Certified in the Governance of Enterprise Technology (GCEIT) – Industry certification, covers security and risk management.

ISACA Certified Information Security Manager (CISM) – Industry certification, covers security and risk management of information systems.

ISC2 Certified Information Systems Security Professional (CISSP) – Industry certification, covers network security, identity and access management, security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations.

Eight common cybersecurity occupations

Penetration Test Engineer

Focus of role

Creates test cases using in-depth technical analysis of risks and typical vulnerabilities and produces test scripts, materials and packs to test new and existing software or services, plans, coordinates and conducts cyber threat emulation activities in support of certification, accreditation, and operational priorities to verify deficiencies in technical security controls.

Titles of roles

Ethical Hacker, ICT Vulnerability Tester, White Hat

Level of responsibility

(SFIA 1-7): 3,4,5,6

SFIA key five skills for this role

Information security (SCTY), Penetration testing (PENT), Security operations (SCAD), Testing (TEST), Vulnerability research (VURE)

Tools and platforms commonly used

- **Penetration testing:** A wide range of software can do this including specialised Linux distributions such as Kali Linux and Metasploit, tools such as Aircrack-ng and Wireshark for packet sniffing, and Nessus and Burp Suite.
- **Vulnerability assessment and scanning tools:** These are designed to look for known vulnerabilities that a malicious actor could use to gain entry to a system or network, such an organisation's public-facing websites. Examples include SQLMap, Nikto, Paros Proxy and Burp Suite.
- **Endpoint detection:** While antivirus software was historically fundamental to a security specialist's ability to combat viruses and malware, it has become supplanted recently with endpoint detection and response (EDR) and extended detection and response (XDR), tools that provide broader capabilities and across both devices and networks. In the case of XDR, boundaries extend to email and cloud deployments.

Technical / IT systems proficiency

(Options: high, medium or low):

High

Programming language proficiency

(Options: mandatory, preferred, not required):

Preferred

Typical qualifications

Bachelor's Degree, Secondary School Education, practical work experience and training

Relevant certifications

Beginner / intermediate

EC-Council Certified Ethical Hacker (CEH) – Industry certification, covers security architecture and engineering, asset security, security and risk management, security assessment and testing, software security and operations.

eLearnSecurity Junior Penetration Tester (eJPT) – Industry certification, this covers assessment methodologies, host and network auditing, host and network penetration testing, and web application penetration testing.

Infosec Certified Cyber Threat Hunter (CCTH) – Industry certification, covers security operations.

Advanced

Comptia+ PenTest – Industry certification, covers hands-on vulnerability assessment, scanning and analysis, as well as planning, scoping, and managing weaknesses.

Offensive Security Certified Professional (OSCP) – Industry certification, covers ethical hacking and penetration testing methodologies using open source tools to demonstrate skills and knowledge.

GIAC Penetration Tester (GPEN) – Industry certification, validates ability to conduct a penetration test using best-practice techniques and methodologies. This includes conducting exploits and detailed environmental reconnaissance..

Expert

Mile2 Certified Penetration Testing Engineer (CPTE) – Industry certification aimed at upper management roles, covers give key elements of Pen Testing; Information Gathering, Scanning, Enumeration, Exploitation and Reporting, covering the latest vulnerabilities and the techniques malicious hackers are using to acquire and destroy data.

Eight common cybersecurity occupations

Cybersecurity Architect

Focus of role

Designs a security system or major components of a security system and may head a security design team building a new security system.

Titles of roles

Enterprise Security Architect, ICT Security Architect

Level of responsibility

(SFIA 1-7): 4,5,6

SFIA key five skills for this role

Consultancy (CNSL), Information security (SCTY), Solution architecture (ARCH), Specialist advice (TECH), System design (DESN)

Tools and platforms commonly used

- **Threat modelling:** These tools allow users to identify and analyse potential risks and attacks their architecture may face. Examples include Microsoft Threat Modeling Tool, OWASP Threat Dragon, and IriusRisk.
- **Secure coding:** These tools help an architect write code free from common vulnerabilities and that follows best practices and standards, as well as apply security principles, guidelines and techniques through the development cycle. Examples include SonarQube, Veracode and Checkmarx.
- **Static and dynamic analysis:** These tools cover analysing code for security issues prior to executing it (static) and then while executing (dynamic) for functionality, performance and behaviour. They also enable an architect to simulate real-world scenarios and improve code quality and maintainability. Examples include CodeQL, Coverity, NDepend (static analysis) plus Burp Suite, ZAP and Nmap (dynamic analysis).
- **Security Architecture Reviews:** These tools help assess an architecture's security across design, documentation and implementation. Examples include SABSA, TOGAF and ISO 27001.

Technical / IT systems proficiency

(Options: high, medium or low):

Medium

Programming language proficiency

(Options: mandatory, preferred, not required):

Preferred

Typical qualifications

Master's Degree, Bachelor's Degree, specialist certifications

Relevant certifications

Beginner / intermediate

GIAC Security Essentials Certification (GSEC) – Industry certification, covers security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations.

SABSA Chartered Security Architect – Foundation Certification (SCP) – Industry certification, covers security architecture and engineering.

Advanced

Cisco Certified Network Professional (CCNP) – Vendor certification, covers network security infrastructure, including concepts, securing the cloud, content security and network security and enforcements.

ISC2 Information Systems Security Architecture Professional (ISSAP) – Industry certification, proves expertise developing, designing and analysing security solutions. Covers architecting for GRC, infrastructure, identity and access management, and applications security.

SABSA Chartered Security Architect – Practitioner Certificate (SCP) – Industry certification. Modules include risk, assurance and governance, architecture design, program and crisis management, business continuity, and investigations architecture.

Expert

CompTIA Advanced Security Practitioner (CASP+) – Industry certification, covers network security, identity and access management, security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations.

ISC2 Certified Information Systems Security Professional (CISSP) – Industry certification, covers network security, identity and access management, security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations.

Eight common cybersecurity occupations

Cybersecurity Engineer

Focus of role

Designs, develops, modifies, documents, tests, implements, installs and supports cybersecurity software applications and systems; ensures they are fully integrated.

Title of roles

ICT Security Engineer, Information Security Engineer

Level of responsibility

(SFIA 1-7): 3,4,5

SFIA key five skills for this role

Information security (SCTY), Release and deployment (RELM), Security operations (SCAD), System design (DESN), Systems installation and removal (HSIN)

Tools and platforms commonly used

- **Networking hardware:** Knowledge around networking hardware such as routers, firewalls and hardware-level security is useful to cybersecurity professionals across many roles including Cybersecurity Engineer. Tools in use to assist here include Secure Boot, TPM, DMA Kernel security mitigation (such as Windows Defender Advanced Threat Protection).
- **Network and systems security monitoring:** Tools used to analyse the status of a network and look for network-centric threats include Nmap, Nagios, Splunk, Argus and OSSEC.
- **Vulnerability assessment and scanning tools:** These are designed to look for known vulnerabilities that a malicious actor could use to gain entry to a system or network, such an organisation's public-facing websites. Examples include SQLMap, Nikto, Paros Proxy and Burp Suite.

Technical / IT systems proficiency

(Options: high, medium or low):

High

Programming language proficiency

(Options: mandatory, preferred, not required):

Preferred

Typical qualifications

Master's Degree, Bachelor's Degree, specialist certifications

Relevant certifications

Beginner / intermediate

EC-Council Certified Ethical Hacker (CEH) – Industry certification, covers security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations.

EC-Council Certified Network Defender (CND) – Industry certification, covers security operations and defence.

ISC2 Systems Security Certified Practitioner (SSCP) – Industry certification, covers asset security, security and risk management, security assessment and testing, software security, security operations.

Advanced

ISC2 – Certified Secure Software Lifecycle Professional (CSSLP) – Industry certification recognising advanced technical skills and knowledge necessary for authentication, deployment, testing, authorisation and auditing throughout the software development lifecycle using best practices, policies and procedures.

ISACA Certified Information Systems Auditor (CISA) – Industry certification, covers security and risk management, security assessment and testing.

Expert

CompTIA Advanced Security Practitioner (CASP+) – Industry certification, this advanced-level cybersecurity certification is for security architects and senior security engineers charged with leading and improving an enterprise's cybersecurity readiness.

Eight common cybersecurity occupations

Cybersecurity Operations Coordinator

Focus of role

Coordinates and responds to complex cybersecurity incidents and hunt investigations, manages tasks across various teams for incident response and hunt operations, advises leadership on operational collaborations and contribute toward strategic planning, facilitates incident response engagements, assesses technical information to develop key messaging.

Titles of roles

Cybersecurity Operations Manager, ICT Security Administrator, Cybersecurity Incident Responder

Level of responsibility

(SFIA 1-7): 1,2

SFIA key five skills for this role

Incident management (USUP), Information security (SCTY), IT infrastructure (ITOP), Threat intelligence (THIN), Vulnerability research (VURE)

Tools and platforms commonly used

- **Network intrusion detection:** Intrusion detection software can detect unusual network or system activity, raising an alarm if a possible threat is found. It can include Kismet, SolarWinds, Security Onion and Snort.
- **Endpoint detection:** While antivirus software was historically fundamental to a security specialist's ability to combat viruses and malware, it has become supplanted recently with endpoint detection and response (EDR) and extended detection and response (XDR), tools that provide broader capabilities and across both devices and networks. In the case of XDR, boundaries extend to email and cloud deployments.

Technical/ IT systems proficiency

(Options: high, medium or low)

Medium

Programming language proficiency

(Options: mandatory, preferred, not required)

Not required

Typical qualifications

Master's Degree, Bachelor's Degree, specialist certifications

Relevant certifications

Beginner / intermediate

Cisco Certified Network Associate (CCNA) – Vendor certification, covers networking fundamentals, configuring IP services, fundamentals in security programs and automation.

CompTIA Security+ – Industry certification, covers asset security, security and risk management, security assessment and testing, software security, security operations.

GIAC Security Essentials Certification (GSEC) – Industry certification, covers security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations.

Advanced

Cisco Certified Network Professional (CCNP) – Vendor certification, covers security infrastructure, including concepts, securing the cloud, content security and network security and enforcements.

GIAC Certified Enterprise Defender (GCED) – Industry certification building on the security skills measured by the GIAC Security Essentials certification. This assesses more advanced, technical skills needed to defend the enterprise environment and protect an organisation as a whole including defensive network infrastructure, packet analysis, penetration testing, incident handling and malware removal.

Expert

ISC2 Certified Information Systems Security Professional (CISSP) – Industry certification, covers network security, identity and access management, security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations.

Day in the life of a cybersecurity professional

Switching careers

Meet Amy

Name: Amy Stirling

Current job: Graduate, Peloton Cyber Security

Years in cybersecurity: 1 year

Formal training and education: Bachelor of Cybersecurity, La Trobe University

I'm a cybersecurity professional because... of the pandemic. I was working as a ski instructor in Japan. The physical wear and tear of skiing full time prompted me to look at alternatives. During one Melbourne lockdown, I looked at the Victorian Government's Free TAFE course list for inspiration, and cybersecurity spiked my interest as it was a topic I'd been conscious of. I was then accepted into a Bachelor of Cybersecurity. Within two weeks, I was equally scared and fascinated by what I learnt. Turns out I did not use safe online practices to protect myself.

A surprising part of the job... is the amount of people in cybersecurity that have come from other industries, particularly those outside of the typical 'corporate' world. It has been a pleasant surprise.

The biggest challenge I've experienced... is the steep learning curve. I was never a kid super into technology growing up and until starting my Bachelor's degree I did not know the name of an ethernet cable.

The reason I love being a cybersecurity professional... is that the work we do is making a difference in reducing the risk companies face while protecting their company, employee and customers' data. This brings me a sense of accomplishment when I see the risk level reducing for our clients.

One unique thing I do every week... would be working on product development. I think it is uncommon for graduates to be working on the sort of tasks I do so early in their career. I am able to provide a fresh perspective as someone without any bias to how something 'should be done'.

I am able to provide a fresh perspective as someone without any bias to how something 'should be done'.

Top tips:

For school or uni leavers:

Be yourself! Whether you are fresh out of school or having a career change, your experience is going to be unique to anyone else's. If you show up as yourself and live your personal values, the right job will come along. Make the most of networking events, whether they are school run or career fairs, attend as many as you can and talk to a range of people there. Make the conversations genuine, not just a sales pitch of yourself – you will meet those people again and it's much nicer if they remember you rather than your resume.

For upskillers or reskillers:

There are so many jobs in cybersecurity that do not involve technical skills so don't let that hold you back. As a professional, there are many transferable skills you can apply. Don't be scared to move beyond your comfort zone – after the fear zone is the learning and growth zones where you may achieve things you never thought possible.

Timeline

- Finishes Year 12
- Becomes a ski instructor and rental technician, working across Australia, Canada, US and Japan for 6 years
- Signs up and completes Bachelor of Cybersecurity at La Trobe University; waitresses part-time while securing degree
- Obtains graduate cybersecurity position at Peloton Cyber Security
- Completes a Diploma in Holiday Parks and Resorts certificate
- Explores Victorian Government Free TAFE course list and develops interest in cybersecurity
- Volunteers with In2Science

Eight common cybersecurity occupations

DevSecOps Engineer

Focus of role

Process monitoring, writing risk analyses, incident management, testing, selection and implementation of technologies, tools and working methods, automation of security controls, control and management of security operations. Role focuses on constructing a "safety culture" within the company by supporting the various teams and customers in the implementation of good safety practices.

Titles of roles

DevSecOps Engineer, DevSecOps Architect, DevSecOps Analyst, Information Systems Security Developer, Cloud Security Analyst

Level of responsibility

(SFIA 1-7): 4,5,6

SFIA key five skills for this role

Incident management (USUP), Information security (SCTY), Methods and tools (METL), Security operations (SCAD), Threat intelligence (THIN)

Tools and platforms commonly used

- **Threat modelling:** These tools allow users to identify and analyse potential risks and attacks their architecture may face. Examples include Microsoft Threat Modeling Tool, OWASP Threat Dragon, and IriusRisk.
- **Secure testing and coding:** These tools help with writing and maintaining code free from common vulnerabilities and that follows best practices and standards, as well as apply security principles, guidelines and techniques through the development cycle. Examples include SonarQube, Veracode and Checkmarx.
- **DevSecOps project management:** This suite of tools is about helping DevSecOps platform maintenance and include continuous integration and delivery/deployment of software development and updates, as well as platform testing, scanning and project collaboration. Examples include GitLab, Tektok Pipelines, Atlassian Bamboo, CircleCI and Travis CI.

Technical / IT systems proficiency

(Options: high, medium or low):

Medium

Programming language proficiency

(Options: mandatory, preferred, not required):

Mandatory

Typical qualifications:

Master's Degree, Bachelor's Degree,Secondary School Education, practical work experience and training.

Relevant certifications

Beginner / intermediate

EC-Council Certified DevSecOps Engineer (CDE) – Industry certification, covers application and infrastructure management of DevSecOps in on-premise and cloud-native platforms.

GIAC Cloud Security Automation (GCSA) – Industry certification, covers understanding of the DevSecOps methodology and toolchains, skill in implementing and configurating security controls throughout automated secure DevOps pipelines.

GitLab Certified DevOps Professional – Vendor certification, covers continuous integration, delivery and the full DevOps lifecycle, managing projects, automating workflows and implementing best practices using GitLab for DevOps.

Advanced

AWS Certified DevOps Engineer Professional – Vendor certification, covers validating technical expertise in provisioning, operating and managing distributed application systems on the AWS platform including process automation, continuous delivery, monitoring and logging. Strong emphasis on principles of DevOps philosophy.

ISC2 Certified Secure Software Lifecycle Professional (CSSLP) – Industry certification showing software development and security professionals have the expertise to apply best practices throughout the secure software development lifecycle. Covers software concepts, lifecycle management, architecture and design, implementation, testing, operations and supply chain.

Expert

CompTIA Advanced Security Practitioner (CASP+) – Industry certification, this advanced-level cybersecurity certification is for security architects and senior security engineers charged with leading and improving an enterprise's cybersecurity readiness.

Eight common cybersecurity occupations

Digital Forensics Analyst

Focus of role

Works on cybercrime investigations, recovering breached, modified or destroyed data, recording and cataloguing evidence related to computer hacks, securing digital storage devices, determining how a hacker gained access to a network.

Titles of roles

Computer Forensic Analyst, Systems Analyst, Malware Analyst, Cyber Defence Forensics Analyst, Cyber Defence Incident Responder, Threat Hunter, IT Auditor.

Level of responsibility

(SFIA 1-7): 3,4,5,6

SFIA key five skills for this role

Digital Forensics (DGFS), Information security (SCTY), Security operations (SCAD,), Threat intelligence (THIN), Vulnerability research (VURE).

Tools and platforms commonly used

- **Forensic analysis:** A range of forensic analysis tools are commonly in the cybersecurity professional's arsenal to assist with identifying, acquiring and analysing electronic evidence in the suspected event of a cyberattack. Businesses also use these to conduct incident response and recover data. For example, organisations can use digital forensics tools to analyse how a breach occurred, whether attackers accessed or exfiltrated data, and how the malicious actors moved through the network. Among these are disk imaging /data capture tools, file viewing tools, network and database forensics tools and analysis tools for file, registry, web, email and mobile device analysis. Examples include Autopsy, Cellebrite, Magnet Axiom, Velociraptor, Microsoft COFEE, and broader disk imaging such as Acronis True Image or ManageEngine OS Deployer.
- **Network and systems security monitoring:** Tools used to analyse the status of a network and look for network-centric threats include Nmap, Nagios, Splunk, Argus and OSSEC.

Technical / IT systems proficiency

(Options: high, medium or low):

High

Programming language proficiency

(Options: mandatory, preferred, not required):

Preferred

Typical qualifications

Master's Degree, Bachelor's Degree, Secondary School Education.

Relevant certifications

Beginner / intermediate

Certified Computer Examiner (CCE) – Industry certification, covers conducting thorough computer investigations, from evidence collection, analysis, to reporting in a forensically sound manner.

Mile2 Certified Digital Forensics Examiner (CDFE) – Industry certification, covers process of detecting hacking attacks and properly extracting evidence to report crime, to conducting audits to prevent attacks.

Advanced

CompTIA Cybersecurity Analyst (CySA+) – Industry certification, covers incident detection, prevention and response through continuous security monitoring.

EC-Council Computer Hacking Forensic Investigator (CHFI) – Industry certification, covers major forensic investigation scenarios, including techniques and standard tools necessary to successfully carry out a computer forensic investigation.

ISACA Certified Information Systems Auditor (CISA) – Industry certification, covers security and risk management, security assessment and testing.

Expert

GIAC Certified Forensic Analyst (GCFA) – Industry certification, covers core skills required to collect and analyse data from Windows computer systems, handling sophisticated incident responses and understanding deep forensic analysis, including the ability to deal with advanced persistent threats.

Certifications

As there are vast bodies of knowledge across many technical specialties and GRC considerations in this sector, generalist and specialist certifications have become a significant part of building a career in cybersecurity. Having certifications on your resume will help you stand out from the crowd and are generally looked favourably upon within the field. Certification may not be expected for entry-level roles, but holding one or more can be a requirement for more senior roles.

A huge range of cybersecurity certifications are available today. These can be divided into vendor and industry certifications, with pros and cons to each. An IT professional, for instance, who has worked in networks and hardware may continue to pursue certifications provided by networking hardware vendors such as Cisco or Citrix that relate to cybersecurity. By contrast, someone who has been on the database or software side may continue to pursue Microsoft. A cloud engineer may choose to continue with AWS or Google, the largest cloud providers in market.

In several cases, industry certifications come in multiple and specialist levels ranging from Entry to Intermediate, Advanced and Expert, such as those provided by ITIL, ISACA, ISC2 and Comptia. Undergraduate university degrees as well as diplomas – both ICT and dedicated cybersecurity – commonly integrate a selection of specific certifications into their programs. But these are usually also available as standalone certifications for school leavers, existing ICT professionals or reskillers who are not undertaking fresh undergraduate degrees in their transition to becoming a cybersecurity professional.

A caveat: Employers will often rate practical application over a list of certifications chalked up in an academic environment, so it's worth being selective in your choices.

ACS also provides recognition through its Certified Technologist (CT) and Certified Professional (CP) programs. These are technology agnostic certifications that recognise transferable skills and competencies held by an IT professional and complement an individual's qualifications, vendor certificates and on-the-job learning with an overarching ACS badge.

At an Advanced level, CT for Cybersecurity applicants must commit to a code of ethics, professional practice and 20 hours of continuing professional development (CPD) per year to retain their status. A combination of minimum academic learning, degree and practical experience is used to ascertain if someone is eligible for CT accreditation, along with in-depth competence in at least one SFIA level 3 specialism such as security administration, service desk and incident management, IT operations, programming / software development and safety engineering.

At an Expert level, ACS CP for Cybersecurity recognises applicants who commit to a code of ethics, professional practice and requires 30 hours of CPD per year. Again, a combination of minimum academic learning, degree and practical experience is used to ascertain if someone is eligible for CP accreditation, along with in-depth competence and 2+ years' experience in at least four SFIA level 5 specialisms including IT governance, information security, security administration, asset management, information management and business risk management.

Several well-known and respected certifications you're likely to come across are listed on the next page.

Employers will often rate practical application over a list of certifications chalked up in an academic environment, so it's worth being selective in your choices.

Beginner / Intermediate

Certification	Type	Focus area
Cisco Certified Network Associate (CCNA) Security	**Vendor**	**Communication and network security**
CompTIA Security+	Industry	Asset security, security and risk management, security assessment and testing, software security, security operations
EC-Council Certified Ethical Hacker (CEH)	Industry	Security operations
GIAC Security Essentials Certification (GSEC)	Industry	Security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations
Google Cybersecurity Professional Certificate	**Vendor**	**Security architecture and engineering**
IAPP Certified Information Privacy Manager (CIPM)	Industry	Asset security
ISC2 Certified in Cybersecurity (CC)	Industry	Security principles, business continuity, disaster recovery and incident response concepts, access control concepts, network security, security operations
ISC2 Systems Security Certified Practitioner (SSCP)	Industry	Asset security, security and risk management, assessment and testing, software security, security operations
ITIL Foundations	Industry	Asset security, security and risk management
Microsoft Certified: Security, Compliance, and Identity Fundamentals	**Vendor**	**Security and risk management, software security**

Advanced

Cisco Certified Network Professional (CCNP)	**Vendor**	**Security infrastructure, cloud, content and network security and enforcement**
CompTIA Cybersecurity Analyst (CySA+)	Industry	Security incident detection, prevention and response through continuous security monitoring
ISC2 Certified Secure Software Lifecycle Professional (CSSLP)	Industry	Technical skills and knowledge necessary for authentication, deployment, testing, authorisation and auditing throughout the SDLC using best practices, policies and procedures
EC-Council Computer Hacking Forensic Investigator (CHFI)	Industry	Computer forensic investigation techniques and tools
EC-Council Certified Cloud Security Engineer (CCSE)	Industry	Security architecture and engineering
GIAC Security Leadership (GSLC)	Industry	Security governance and technical controls, security lifecycle management
Infosec Certified Cyber Threat Hunter (CCTH)	Industry	Security operations
ISACA Certified in Governance of Enterprise IT (CGEIT)	Industry	Enterprise IT governance and resource management
ISACA Certified in the Governance of Enterprise Technology (GCEIT)	Industry	Security and risk management
ISACA Certified Information Systems Auditor (CISA)	Industry	Security and risk management, security assessment and testing
Offensive Security Certified Professional (OSCP)	Industry	Security operations
SABSA Chartered Security Architect Practitioner certificate	Industry	Security architecture and engineering

Expert

Cisco Certified Internetwork Expert (CCIE)	**Vendor**	**Network technology and solution leadership**
CompTIA Advanced Security Practitioner (CASP+)	Industry	Network security, identity and access management, security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations
GIAC Certified Incident Handler (GCIH)	Industry	Security operations
GIAC Security Expert (GSE)	Industry	Network security, identity and access management, security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations
ISACA Certified Information Security Management (CISM)	Industry	Security and risk management and leadership
ISC2 Certified Information Systems Security Professional (CISSP)	Industry	Network security, identity and access management, security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, security operations
Mile2 Certified Penetration Testing Engineer (CPTE)	Industry	Pen testing; information gathering, scanning, enumeration, exploitation and reporting
SABSA Chartered Security Architect - Master	Industry	Security architecture and engineering

Day in the life of a cybersecurity professional

The value of information

Meet Sudheera

Name: Sudheera Edirisinghe

Current job: Associate Director of Cybersecurity, Optus

Years in cybersecurity: 15

Formal training and education: CISSP, CCSP, SABSA and CEH qualifications, number of cybersecurity-related certifications from other institutions.

I got into cybersecurity because... of inherent curiosity. As a fan of sci-fi and thriller movies, shows like Star Trek and The Net played a significant role in inspiring my career choice. Over the years, I came to realise the profound importance of digital systems and value of information stored within them, and the potential impact of mishandling such systems. I initially concentrated on learning how potential adversaries could compromise these systems by trying to think like a potential adversary. This interest ultimately led me to focus on securing these systems.

A surprising part of the job... is there's no silver bullet solution. A piece of advice I received early on still holds true: As 'good guys', we must consistently get it right, whereas the 'bad guys' only need to succeed once for an impactful breach. This wisdom remains relevant and resonates with me to this day.

The reason I love being a cybersecurity professional... is no two days at the same. Adversaries continually shift their tactics, armed with ever-evolving techniques. Being prepared to bring your 'A' Game consistently is crucial. It's essential not to hesitate in embracing new knowledge.

A career highlight... was playing a significant role in establishing cybersecurity as a formalised function within my organisation, where I developed cybersecurity policies and a governance structure. I delivered cutting-edge solutions to defend the company, some of which were pioneering in the industry.

One unique thing I do every week... involves consistently incorporating lessons learned to enhance our safeguards. We like to rely on playbooks when responding to incidents, so our approach is consistent and measured and ensures steps are not missed.

No two days at the same. Adversaries continually shift their tactics, armed with ever-evolving techniques.

Top tips:

For school or uni leavers:

It's essential not to let hype be the sole motivation for entering this field. Succeeding in cybersecurity requires a commitment to investing extensive hours for mastery. Passion for the chosen career path is crucial, and possessing traits such as resilience and a willingness to learn are key factors that contribute to long-term success.

For upskillers or reskillers:

Acquiring knowledge about the functioning of computer and network systems is undoubtedly beneficial. Proficiency in comprehending how systems operate motivates individuals to devise best forms of defences against potential cyber threats. However, it's essential not to discourage individuals from entering the profession, especially new starters. If you possess strong problem-solving abilities, analytical skills and demonstrate a keen aptitude for learning and hard work, you may well be the ideal candidate sought after in our field. This industry values individuals with diverse backgrounds.

Timeline

- Starts career as a Systems then Network Engineer in the private sector
- Completes a Bachelor of Computing and Information Systems at University of London
- Joins Optus as IP Network and Security Designer, then becomes Firewall and Security Design Manager
- Obtains Masters in Business and Technology, AGSM
- Gains a range of cybersecurity certifications, starting with vendor certifications, then several SABSA and ISC2 accreditations
- Promoted at Optus to cybersecurity, helps set up first governance organisation to manage cyber risk
- Gains CCSP status in Cloud Security, as well as Cyber Risk Management at La Trobe University

Cohort guidance

Formal learning pathways into cybersecurity

School leavers + reskillers

As we have already noted, one of the primary formal pathways into a cybersecurity career is completing a university undergraduate degree – either in ICT, cybersecurity or a similar course designed to equip you with the education and foundational technical skills to get a job in the industry. This is not an exhaustive and complete guide, and the ACS recognises these will change and shape-shift. For an updated list of ACS accredited course, visit: acs.org.au/cpd-education/accredited-courses.html

Examples of formal undergraduate degrees include:

- Bachelor of Cybersecurity, Deakin University (VIC)
- Bachelor of Science (Cybersecurity), Edith Cowan University (WA)
- Bachelor of Computing and Cybersecurity, UNSW Canberra (ACT)
- Bachelor of Cybersecurity / Bachelor of Criminolog, La Trobe University (VIC)
- Bachelor of Information Technology (Networking and Cybersecurity), University of Technology Sydney (NSW)
- Bachelor of Information Technology (Networking and Cybersecurity), University of South Australia (SA)
- Diploma of Cybersecurity, Torrens University Australia (SA)

Course length varies between institutions, but typically expect three years. ATAR requirements can range between 50 to 90, with many in the 50 to 70 range.

Expectations of prior education can greatly vary from institution to institution, but high school subjects such as maths and information technology are viewed favourably and often considered alongside the ATAR score for entry for high school leavers.

Uni graduates + ICT upskillers

For existing ICT / STEM graduates or ICT professionals looking to upskill, a Master's, postgraduate degree or diploma may be an alternative pathway to building your cybersecurity formal credentials and knowledge. If you're already working in ICT or have a degree in a related field, such as a Bachelor's degree in computer science or a field such as maths or engineering, your experience and knowledge are transferable.

Selection is usually based on minimum course entry requirements. These comprise holistic consideration of your academic merit (such as completing a Bachelor's degree in another domain or related discipline), relevant work experience, likelihood of success, availability of places, participation requirements, regulatory

Course name	Provider	Cohort
Certified Cybersecurity Professional	Lumify Learn	School leaver / uni graduate / upskiller / reskiller
Graduate Certificate in Cybersecurity Management	University of Canberra	School leaver / uni graduate / upskiller / reskiller
Certificate IV in Business (Cybersecurity)	Swinburne University Open Education	Uni graduate / upskiller / reskiller
Cybersecurity Career Starter course collection	Learning People	School leaver / upskiller / reskiller
Graduate Certificate in Data and Cyber Management	Ducere Global Business School	School leaver / uni graduate / upskiller / reskiller
Certificates and diplomas in cybersecurity	TAFE	School leaver / uni graduate / upskiller / reskiller
ISC2 Certified in Cybersecurity	Industry	School leaver / uni graduate / upskiller / reskiller
ITIL Foundations	Industry	School leaver / uni graduate / upskiller / reskiller
Microsoft Certified: Security, Compliance, and Identity Fundamentals	Vendor	School leaver / uni graduate / upskiller / reskiller
ISC2 Certified Information Systems Security Professional (CISSP)	Industry	Upskiller
Mile2 Certified Penetration Testing Engineer (CPTE)	Industry	Upskiller
SABSA Chartered Security Architect – Master	Industry	Upskiller

requirements and individual circumstances. In the case of cybersecurity, related disciplines range from network security experience to hardware, forensics, and broader IT engineering experience. Commonly, students also need to pass English language proficiency requirements to secure a place in a Master's program.

Examples of these include:

- Master of Cybersecurity, Deakin University
- Master of Cybersecurity (Professional), Deakin University
- Master of Cybersecurity, Edith Cowan University
- Master of Cybersecurity, University of Southern Queensland
- Master of Cybersecurity, Charles Sturt University

Content of these courses can vary greatly from institution to institution, but you will find they will teach you subjects ranging from application development and data analytics, to network design and security risk analysis, cryptography and digital forensics and everything in between. Cybersecurity cuts across many ICT fields, so expect wide and varied topics to sink your teeth into.

Often experience in the industry, or in an aligned industry, is considered too. It can support your application for a course, especially if you're a mature age student or changing careers.

Alternative education pathways: School leavers + reskillers

With more than half of Australia's current cybersecurity professionals lacking any tertiary qualifications, it's clear there are opportunities for those who have not gone to university to get into cybersecurity.

So can you teach yourself cybersecurity well enough to find employment? There is certainly enough freely available information online to learn what you would need to know, and networking may open some doors. But without a certificate demonstrating institutional education or a cybersecurity certification, you may find it hard to get anything but the most entry-level positions.

Boot camps and accelerated graduate programs are additionally on offer from several universities, although they're pricey. Take University of Sydney's Cybersecurity Bootcamp collaboration with EdX, available part-time, or RMIT Online's Graduate Certificate in Cybersecurity in collaboration with Palo Alto Networks. Both can be achieved in under one year.

Alongside graduate courses, you can pursue an education through VET (vocational education and training) for cybersecurity. Like graduate certifications, these provide an alternative and often more hands-on, fast-tracked learning pathway and experience.

Another path forward is leveraging microcredentials to certify your skills or experience. Microcredentials are offered by universities, professional bodies and other learning institutions and are officially endorsed by the Australian Government through the National Microcredentials Framework. ACS offers cybersecurity microcredentials, including Cybersecurity – Information Security; Cybersecurity – Compliance and Assurance; Cybersecurity – Intrusion Detection; and Cybersecurity – Identity and Access.

Microcredentials can be useful for those who are already employed and don't have a lot of time to study but wish to expand and certify their skills. Useful education resources to help you find degrees, VET courses and microcredentials include:

- yourcareer.gov.au (including My Skills)
- www.courseseeker.edu.au
- www.microcredseeker.edu.au

Currently, experience and exposure are more highly prized by industry and employers. Cybersecurity is a constantly evolving landscape, and on-the-job experience will take you far when you apply for a role and attend an interview.

But when it comes to plotting a path to higher paying roles, specialisms are going to be critical. This doesn't mean you can't mix it up – for example, start in a more technical role then move into GRC positions. Cybersecurity provides for a wide range of options, given disciplines and the specialisms beneath them often cross over and draw on each other.

Although more senior roles often require one or more certifications as well as experience in the field itself or a related one, with a little cross-skilling, you can move from one field of practice to another within a cybersecurity discipline, depending on where your interest and experiences take you.

Prior experience in the industry is required to attempt to gain certification in some cases, such as with the more advanced CISSP certification. However, cybersecurity builds upon the foundations of ICT, crossing a wide range of skill sets. If you have experience in one facet of ICT, it's very likely to be transferable to cybersecurity, and you can certify your abilities through channels such as microcredentials. When it comes to getting into the industry and your chosen specialisation, experience and microcredentials can make you a compelling candidate.

For example, experience working in helpdesk, systems admin, networking infrastructure, desktop tech or as a support engineer can translate into a cybersecurity specialisation quite easily. Most of this experience falls under the cybersecurity purview. Take the work of deploying desktops: This will require security and group policies to be applied. Hardware security also requires configuration and customisation.

Any IT professional that touches on user permissions, system privileges, access control, traffic monitoring and filtering has experiences perceived to be security related.

Extra considerations for migrants

For migrants coming into Australia looking to pursue a career in cybersecurity, additional conditions must be met, particularly if you're hoping to be considered for roles within Australia's public sector. The first relates to citizenship and security clearance.

While it is possible to get temporary work in Australia's public sector as a non-AU citizen, The Australian Public Service Act requires agencies not to engage an employee who is not an Australian citizen, unless the Agency Head considers it appropriate to do so. In considering the appropriateness of waiving citizenship requirements, the Agency Head may consider factors including the agency's internal policies, its security environment, and the specific requirements of the role. Similarly, the APS employment framework allows each agency to impose and manage conditions of engagement, including security and character clearances.

If you are not an Australian citizen, the minimum requirement is you must be eligible to work in Australia and hold a valid work visa. Prospective Australian Public Service (APS) employees may also be asked if they are willing to undergo a security clearance. You must be an Australian citizen to be eligible for a security clearance. This is also the case for roles in organisations providing services to the APS or Defence Australia.

Given the time taken to achieve permanent residency, then Australian citizenship, this can delay a candidate's ability to work in a dedicated APS or Defence cybersecurity position for several years. For example, anyone wishing to become an Australian citizen needs to have resided lawfully in the country for a minimum of four years before being eligible, including 12 months as a permanent resident.

The good news is Australia recognises ICT security as a priority skilled migration occupation, which means individuals immigrating with former proven field experience can be given higher priority in the visa application process. Categories of visa described as the most practical for ICT security professionals are: 190 Skilled Nominated Visa and 491 Skilled Regional (Provisional) Visa. The common starting process to achieving these is to firstly seek professional migration advice about eligibility for Australian immigration, obtaining a satisfactory English test, and obtaining a satisfactory skills assessment. Many ICT skill assessments including those for ICT security are undertaken by the ACS.

For ICT professionals hoping to gain dedicated cybersecurity employment, several ICT skilled roles also fit into priority professions. These could provide a step onto the cybersecurity career path long term. Examples include Computer Network and Systems Engineers, Programmers and ICT Project Managers.

For those looking to migrate as students, increasingly stringent rules are in place, more broadly around student visa eligibility but also specifically pertaining to ICT areas of study. Under the newly activated Migration (Critical Technology - Kinds of Technology) Specification, effective 1 April 2024, the Federal Government can apply additional pre-visa screening for postgraduate studies and has the power to refuse or cancel visas if it fears applicants present "an unreasonable risk of unwanted critical technology knowledge transfer".

The Australian Government has identified seven critical technologies to 2030, including advanced information technologies, artificial intelligence and advanced computing. These new additional visa conditions may have a bearing on postgraduate studies and should be reviewed before commencing the visa process to migrate to Australia.

For more information, visit:

Ausdirect Migration agency

ausdirectmigration.com/how-to-migrate-to-australia-as-an-ict-security-specialist/

View online

ACS

www.acs.org.au/msa/information-for-applicants.html

View online

Australian Public Service Commission

www.apsc.gov.au/working-aps/information-aps-employment/guidance-and-information-recruitment/citizenship-aps

View online

Australian Government Security Vetting Agency

www.agsva.gov.au

View online

Latest Federal Government Migration Specification

www.legislation.gov.au/F2024L00182/latest/text/explanatory-statement

View online

Day in the life of a cybersecurity professional

Climbing the ladder

Meet Robin

Name: Robin Poudel

Current job: Cybersecurity Analyst, Cythera

Years in cybersecurity: 2 years

Formal training and education: Diploma in IT, Bachelor of Computer Science majoring in cybersecurity; ISC2 Certified Cybersecurity (CC); CCNA (Cisco Certified Network Associate)

I got into cybersecurity because… I've been interested in cybersecurity since I was 16 years old. I got into a bit of trouble as a kid – I think every cybersecurity professional has a story of something they shouldn't have done. I learnt technologies and tools that can be used to exploit things, watched YouTube videos, read books and journals and built skills from there. I wanted to be a pen tester/hacker.

A surprising part of the job… is the amount of training. Cythera invested in 3-4 months of training for me to get started on triaging events. Training can be challenging and can get a bit boring as you're not doing the actual work. Patience is important in this career.

The reason I love being a cybersecurity professional… is the satisfaction you get when you're able to defend organisations using tech in their everyday lives. Think of your favourite restaurant or retail shop – they need to be defended. The tools and technologies we use are also rewarding. I couldn't imagine we could do these things when I first started and said to my manager, 'you can really do this? And dig this deep into the user's device? And do this kind of investigation?'.

A career highlight… was an active, very large incident we worked on that I was shadowing, where the event could have been exploited heavily. We were able to stop it happening before it reached the level of data breach events like those we've seen occur at Optus or Medibank.

One unique thing I do every week… is use previous knowledge from technical roles when triaging events as attacks evolve. Threat actors trying to hack into systems are evolving and becoming very creative. That presents us with something new every day.

> I am able to provide a fresh perspective as someone without any bias to how something 'should be done'.

Top tips:

For school or uni leavers:

You will go to the top if you're capable, but it's important to climb the ladder. Find something you can leverage, such as a helpdesk or support roles. There are platforms to test and learn with too, such as Hack The Box and TryHackMe. But don't stand in two boats at the same time – you'll end up falling in sideways. Stick to one boat, try to sail it first. You don't have to learn everything in three days. And if you can, invest in your own home lab as it'll let you try things. If you don't break things, you won't learn.

For upskillers or reskillers:

Find things within the organisation where you can support and learn from what other teams are doing. There's no harm in being friends. Ask to shadow for an hour and see what interests you most. Ninety per cent of people won't mind teaching your things.

Timeline

- Finishes Year 12
- Migrates to Australia from India as an international student to do Bachelor of Computer Science, majoring in Cybersecurity
- Gains internship as IT Helpdesk Operator at Brighton College Australia, moves on to network administration
- Becomes ACS, ISACA, Australian Information Security Association member
- Completes professional year of IT at Monash University; certifies in ISC2 for Cybersecurity and CCNA
- Completes various online free courses on LinkedIn, Lynda.com, NABSA, ANZ, Skillsoft, RangeForce
- Gets job as Cybersecurity Analyst at Cythera

Landing a job in cybersecurity

If it's your first role and you're building experience in cybersecurity, you'll need to start in entry-level positions, such as Junior Security Specialist or Associate Cybersecurity Analyst. We've already covered the pros and cons of having relevant certifications, microcredentials and other education, training and work experiences, to get into the cybersecurity space. But just like any role you may apply for, highlighting your knowledge, strengths and experiences against stated criteria, while keeping it succinct, is key.

When it comes to the interview, you may be tested on your knowledge and abilities on the spot. Some organisations may pose interview questions to gauge not only your aptitude in a given field, but also your general ability to problem-solve. To this end, you may be given potential scenarios or asked to demonstrate solutions to a problem to see how well you think outside of the box.

"To help our recruitment processes at Domino's, we came up with a mini-hacking challenge, the idea of which was to test a candidate's ability to find things out. You didn't have to have any experience at all and were guided enough that if you did some searching, and you were persistent, you'd be able to unlock all levels of the challenge. When you finished it, you got a secret email address to apply. Then you had to document exactly what you did in a report. The person who got the job, a former delivery driver, was against people internally who worked in the IT team and who, on paper, were more qualified. But the candidate's report was amazing: It had screenshots and a really strong narrative. That sealed the deal even before we met them. It really showed attention to detail."

Stephen Bennett
CISO, Domino's

You may also need to go through multiple interviews. Don't forget this is your opportunity to interview your potential employer – is this a place you would want to work? What kind of projects could you be working on? Who would you be working with? Come prepared with questions, especially about the organisation itself.

Finally, to get an idea of what you might be asked in advance, Google typical questions used in prior interviews. If nothing else, this can help you prepare by getting you to think about subject focus and what you might be able to talk about to sell your abilities. Questions you could be asked include:

- How do you define the differences between encoding, encryption and hashing?
- What is your process to prevent identity theft?
- What is an emerging threat in cybersecurity that deserves more attention?

Or, to make it more difficult, you may be asked questions such as:

- What is a polymorphic virus?
- Can you describe the process of salting?
- Can you give an example of social engineering?

Questions used in higher-level job interviews can be more scenario-based and require examples of where and how you have achieved certain outcomes. These aim to get candidates to describe a situation, explain the task, specify actions they took and detail any results (STAR, standing for situation, task, action and result):

- You discover a security breach in a company's network during a penetration test. What immediate steps would you take to contain the breach, investigate the incident, and prevent future occurrences?
- Tell me a time where you went beyond above and beyond your job duties when faced with a challenging situation at work?
- Share a time when you had to persuade a client or co-worker to go in a different direction?

"We took a Queensland TAFE student and put them on a 360-degree work experience program to play in all the different cyber spaces. We then took them on as an employee in our capability team, which is a good place to learn the craft of cybersecurity. You're not homed into anything, you're really wide because you're quoting up all different sorts of engagements. Understanding your personal passion helps you in this career, as well as knowing what you need. It helps to start articulating those so me as the business owner can say, 'you want to be here but actually, you look like you can sit in these roles and why don't we try before we buy'."

Angela Champion
CEO and Co-Founder, White Rook Cyber

In addition to qualifications and certifications, familiarity with the NIST Cybersecurity Framework would be an excellent addition to your resume. The framework is, in its own words, 'Voluntary guidance based on existing standards, guidelines and practices for organisations to better manage and reduce cybersecurity risk'. It's a product of the National Institute of Standards and Technology (NIST), a US Government organisation, and favourably regarded worldwide as it can be applied to any business or institution with respect to quantifying and mitigating cybersecurity risks. Several employers list a preference for familiarity with the framework.

A caveat here is other frameworks exist and may be more appropriate depending on an organisation's requirements. These include SFIA or ISO 27002. It's worth checking if one of these is more applicable to the position you're seeking, or when exploring public versus private sector roles.

You may additionally want to familiarise yourself with Australian cyber frameworks, especially if you plan to work for the Australian Government.

Created by the Australian Cybersecurity Centre (ACSC), these are part of the Australian Signals Directorate. Frameworks most often referenced include the Essential Eight, a set of guidelines and checklists for businesses and government agencies to protect themselves from cyber threats; plus ASD ISM (Information Security Manual).

There is also the ASD Top 35 Mitigation Strategies, listing 35 different ways organisations can and should protect themselves.

For more, visit: cyber.gov.au

Graduate, internship and work experience

There are plenty of graduate roles about in cybersecurity and broader ICT within the private sector. Many employers prefer – but do not require – hands-on ICT, network, vendor platform or security-related experience. Minimum requirements commonly involve Australian citizenship or permanent residency status.

In larger private consulting houses and services-based organisations, employers have a heavy emphasis on people skills and will be looking for individuals who are self-starters, have great communication skills, can problem solve and think out of the box, have a can-do attitude, and collaborate and work well in a team.

Full-time or part-time graduate positions are open to those who've just completed or are completing their final year of undergraduate or postgraduate study, in a relevant discipline such as Cybersecurity, Technology, Computer Science and Information Systems.

For more graduate examples, check out:

GradConnection

au.gradconnection.com/graduate-jobs/cyber-security/australia/

View online

Seek

seek.com.au/cyber-security-graduate-jobs

View online

Ernst & Young

ey.com/en_au/careers/cybersecurity-student-opportunities

View online

Australian Defence Force

army.adfcareers.gov.au/jobs/communication-it-and-intelligence

View online

At ACS, we champion the technologies, people and skills critical to Australia's future.

We create value for our members, businesses and society by providing community, advocacy and professional development.

Contact us

Member services general enquiries
T: +61 2 9299 3666
E: member.services@acs.org.au

Canberra
acs.canb@acs.org.au

New South Wales
acs.nsw@acs.org.au

Northern Territory
acs.nt@acs.org.au

Queensland
acs.qld@acs.org.au

South Australia
acs.sa@acs.org.au

Tasmania
acs.tas@acs.org.au

Victoria
acs.vic@acs.org.au

Western Australia
acs.wa@acs.org.au

acs.org.au