

Cyber Security in Australia: Training for Cyber Resilience and the Fourth Economy



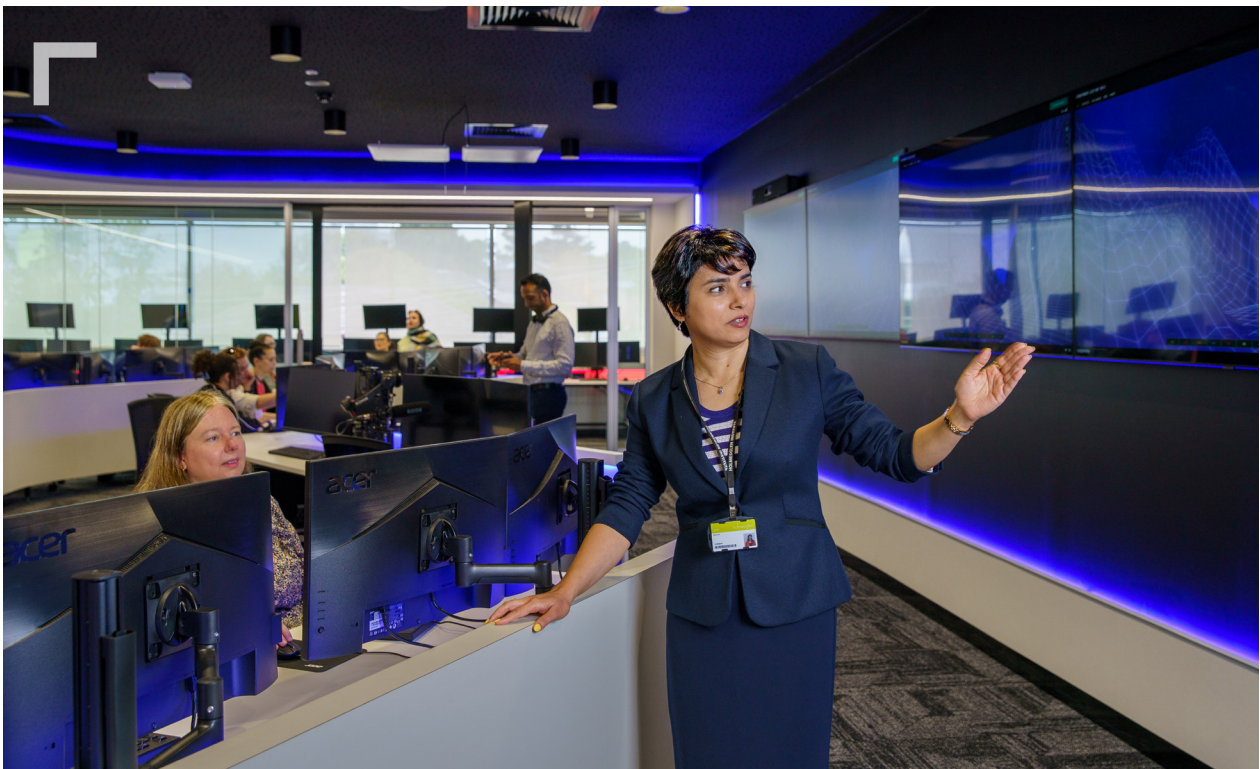
Introduction

Australia today stands at a cyber security crossroad. It faces an evolving threat landscape while pursuing an ambitious national goal to be a global cyber security leader by 2030.

This **In Focus** white paper provides insights from Holmesglen Institute's student data and cyber security team. Aligned to Australia's Strategic Framework, Holmesglen's analysis offers a path forward for cyber security training – a key pillar in strengthening cyber resilience across all sectors of our society.

Purpose

This white paper serves to contribute additional data and insight to Australia's national discussion about cyber security resilience through a prism of skills acquisition, training and delivery. To do this, Holmesglen chiefly draws on its own student data, TAFE sector data from the National Centre for Vocational Education Research (NCVER), third party employment data and analysis from its cyber security team.



Summary of Key Findings

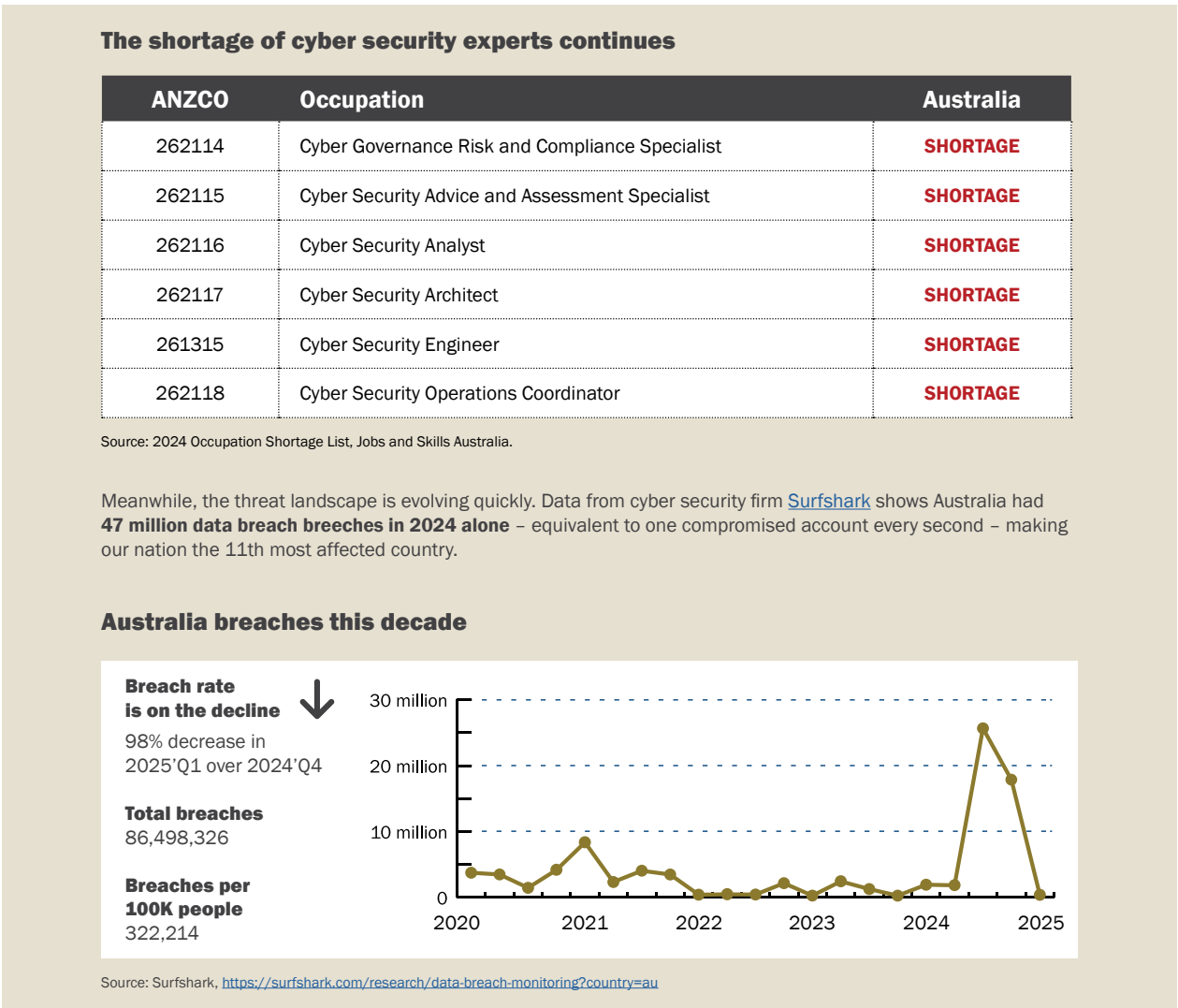
- Holmesglen's cyber security student cohort is predominantly male career changers, with increasing participation from women and mature workers helping to address skill shortages.
- Holmesglen has contributed a steady number of Certificate IV in Cyber Security graduates over the past five years.
- A more responsive curriculum and nimble microcredential delivery is expected to support future growth, boost completions and increase job prospects.
- Our students' satisfaction rates are very high due to Holmesglen's strong market differences, suggesting TAFE courses in this space remain trusted despite readily available non-accredited private training options.
- Employment and further training outcomes for TAFE cyber security graduates are above the TAFE average.
- TAFE-delivered industry certifications, such as microcredentials and short courses, are expected to give students an edge over other job applicants.
- The median salary for a cyber security worker in their first role generally falls within a broad range, with Certificate IV in Cyber Security graduates earning slightly more than the TAFE average.
- More awareness about the value of TAFE cyber security courses among recruiters may help lift graduate salary outcomes even further.
- TAFE, industry, and government can work together to update training packages faster and problem-solve through applied research.
- Cyber security training trends are emerging in teaching practice, flexible delivery, collaborative platforms, fast to market microcredentials and greater industry engagement.
- Students learning cyber security can differentiate themselves by building a strong resume, strong portfolio, real client experience, a sense of community and professionalism.
- Employers are prioritising five critical skills and attributes; relevant qualifications and certifications, technical skills, problem solving, adaptability and teamwork.

TAFE, industry, and government can work together to update training packages faster and problem-solve through applied research.

Situation

While estimates vary, in 2023 [AustCyber \(now Stone & Chalk\)](#) calculated that the local cyber security sector would need **an extra 4,813 dedicated roles annually** just to meet demand for 2030. When Oxford Economics Australia analysis was applied, the estimate grew to **potentially 85,000 roles** or an increase of 66% on 2023.

Today, employers remain unable to fill, or have considerable difficulty filling, vacancies at current levels of remuneration, conditions and locations for the six cyber security occupations tracked by [Jobs and Skills Australia](#). We note that by this list which is tracked over time, the occupation shortage has generally not abated significantly since 2021.



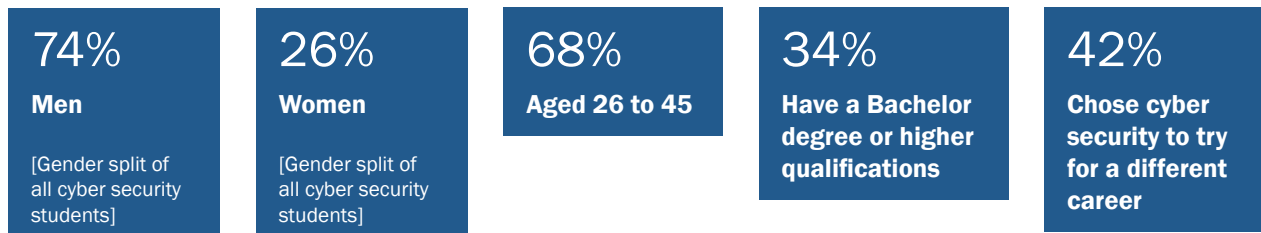
The rise of ransomware

Ransomware has emerged as a dominant threat vector. Australian organisations pay an average USD\$6 million per incident, 50% higher than the global average according to [Sophos Ransomware](#). [CFC Underwriting](#) notes that these attacks now account for 89% of total cyber-related business costs for Small to Medium Enterprises (SMEs) in Australia over the past 12 months. These reports reflect attackers' strategic focus on disrupting operational continuity. SMEs face disproportionate risks, with 60% reporting cyber security incidents cost an average of AU\$50,000 for small businesses and AU\$63,000 for medium organisations (Australian Cyber Security Centre in [Insurance Asia](#), April 2025).

Lastly, in recent times we have seen Australia's healthcare sector experience particularly severe impacts from cyber security incidents. Office of the Australian Information Commissioner ([OAIC](#)) says the MediSecure breach exposed data of **12.9 million people** – the largest single incident since the Notifiable Data Breaches scheme began.

Most Holmesglen cyber students are male; some have degrees and many are reskilling

Our enrolment data shows a skew toward male learners, comparable to the composition of IT student cohorts in other published studies, with only a quarter being female. (We note that this is however nearly 10% higher than the estimated percentage of women to men working in the cyber security according to a [2023 Australian Government](#) report.) Most of Holmesglen's cyber security students are in their early to middle career stage. It is salient that two-thirds have no higher qualification and a large volume are reskilling.



Source: Enrolled Holmesglen students across all cyber security courses 2021-2024.

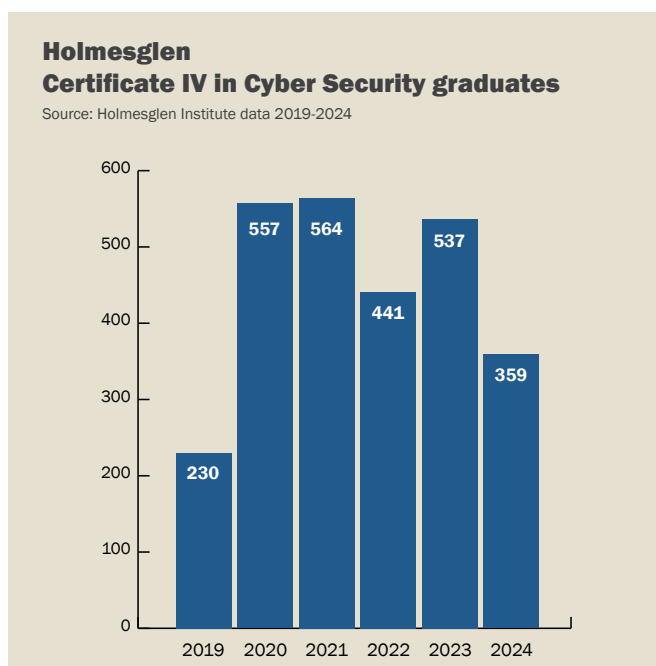
Analysis

- Supporting more women to study cyber security could help alleviate the nation's crucial skills shortage.
- Training providers, industry and schools can work together to make cyber security more accessible.
- Encouraging those aged 45+ to acquire short course skills may reduce barriers and tap into this cohort.

Holmesglen has contributed a steady number of quality graduates over the past five years

Since introduced in Semester 2, 2018, our Certificate IV in Cyber Security has delivered a steady volume of graduates with a total of 2,688 students completing to the end of 2024. (Our 2024 data shows a short term reduction due to enrolment cycle and course changes.)

Course and delivery updates are expected to support future growth and outcomes.



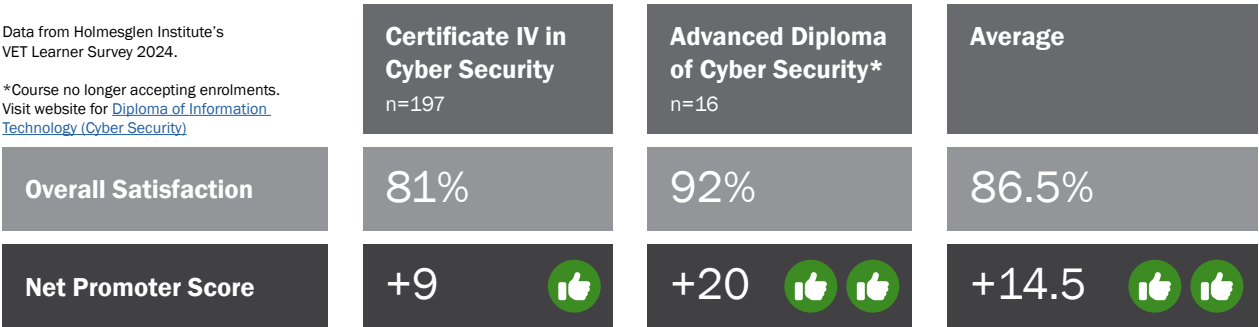
Analysis

- Changes in 2025, requiring the Certificate III in Information Technology for Free TAFE eligibility, will support growth and boost future completions.
- New microcredential skill sets in essential Cyber Security training plus Holmesglen's Bachelor of Information Systems provide a rounded learning pathway for graduates.

Overall satisfaction among Holmesglen’s cyber security students is very high

Recent Holmesglen data shows very high levels of overall satisfaction among our cyber security students, with similarly strong Net Promoter Scores. Like other providers we deliver to the same national training package.

We therefore consider these results to be a fair indicator of our market differences, notably our industry links, job outcomes, teaching quality, new CSOC facility, flexible study mode and learner support.

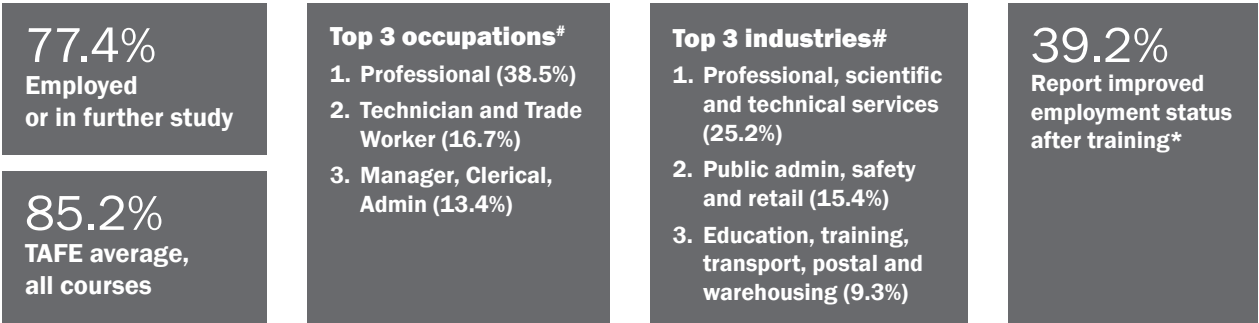


Analysis

- Today’s students still place great value in a quality training experience from a trusted provider offering a mix of conveniences and strong job outcomes.
- Despite a proliferation of readily accessible and non-accredited private provider short courses, TAFE training in cyber security certificates, diplomas and IT degrees remains highly competitive in market.

TAFE cyber security graduates experience good employment outcomes

Overall, Certificate IV in Cyber Security graduates enjoy solid employment or further study outcomes with almost 40% of those employed going into professional roles and the balance technician positions. Despite this, only 39.2% reported improved employment status.



*Source: NCVER 2024 data combining Certificate IV in Cyber Security previous course 22334VIC and current course 22603VIC. # Of those employed after training

Analysis

- TAFE-based cyber security training is strongly supporting Australian employers to fill critical skills gaps at the technician, professional and managerial levels across diverse sectors.
- An opportunity exists to educate the wider community about TAFE’s key training role in supporting Australia’s Cyber Security Framework with a view to further improving employment status for graduates.

EXPLAINER 1

Skills, jobs and study pathways for TAFE cyber security training



Certificate IV in Cyber Security	Diploma of IT (Cyber Security)
Skills and capabilities Identifying and reporting: • System vulnerabilities • Website threats • Cyber incidents Practical skills in: • Pen testing • Network security • Firewall management • Web security • Python programming	Skills and capabilities • Industry certifications in cyber security, cloud computing and system administration • Secure networks • Manage IT systems • Deploy cloud solutions • IT support and network security
Work after study • Cyber security support officer • Desktop support technician • Cyber security intrusion tester • Security support officer • Security PEN tester • Network security support officer • Computer forensics technician • Website security support officer	Work after study • Network Security Specialist • Systems Administrator • Cloud Engineer • IT Support Specialist • Cyber Security Analyst • Cloud Security Engineer • Security Engineer • Cyber Security Incident Responder
Further study pathways • ICT50220 Diploma of Information Technology • BIS24 Bachelor of Information Systems	Further study pathways • BIS24 Bachelor of Information Systems • A range of other IT related Bachelor qualifications

Source: [Holmesglen Institute Centre for Cyber Security and Digital Information Technology](#)

EXPLAINER 2

Australian Government Strategic Framework: The Six Cyber Shields



Australian Government

“Each shield provides an additional layer of defence against cyber threats and places Australian citizens and businesses at its core. Throughout the period covered by the 2023–2030 Australian Cyber Security Strategy (the Strategy), the Australian Government will work with industry to reinforce these shields and build our national cyber resilience.”

Source: [2023-2030 Australian Cyber Security Strategy](#), p.6

How Holmesglen is contributing



SHIELD 1: Strong Businesses and Citizens

- 1. Ensuring the next generation is cyber aware.**
Programs such as the Certificate III in Enabling Technologies develop foundational cyber security skills in high school students.
- 2. SME focused cyber security certifications and microcredentials.**
Delivering fast to market, responsive training that builds capabilities of workforces.
- 3. Applied hands on learning through the Training CSOC and Cyber Range.**
Ensuring businesses are secure and see value in implementing training for their staff, notably where they have early identification phishing attacks.
- 4. Developing cyber security professionals through qualifications and certifications.**
This includes the Certificate IV in Cyber Security and the Diploma of Information Technology (Cyber Security).



SHIELD 2: Safe Technology

- 1. Purchasing technology** from our supply chain which adopts cyber security standards.
- 2. Early adoption** of governance policy and guidelines supporting ethical use of generative AI.
- 3. Internal policy and guidelines:**
 - Artificial Intelligence Operational Policy
 - Generative Artificial Intelligence Guidelines



SHIELD 3: World Class Threat Sharing and Blocking

- 1. Reporting of cyber security incidents** (real-time data enables government to detect attack patterns and preemptive threat blocking).
- 2. Collaboration with government** agencies to continuously enhance our security posture.



SHIELD 4: Protected Critical Infrastructure

- 1. Incident testing** at regular intervals.
- 2. Cyber security competency** and governance improvements.



SHIELD 5: Sovereign Capabilities

- 1. Cyber security training** to upskill the workforce and encouraging technology innovation in Australia:
 - Cyber security qualifications
 - Industry certifications
 - Microcredentials



SHIELD 6: Resilient Region and Global Leadership

- 1. Supporting government targets** to supply industry with professionally trained workforces.

TAFE graduates in cyber security are well-positioned to earn attractive entry-level salaries.

Certificate IV in Cyber Security graduates can command good first full-time salaries in the sector, slightly above the TAFE average according to 2024 NCVER Student Outcomes Survey data. While lower than the median salary of a university undergraduate completer, these TAFE graduates can increase their salary over time with workplace experience, applied research and adding higher qualifications.

When we consider a broader range of published upper end salary data combining first role and early career cyber security roles, we get an approximate average salary of **\$102,400 pa**. This is a potentially achievable target for a TAFE cyber security graduate with the right mix of experience and skills.

Median First Role Salaries in Cyber Security				Comparison Median Salaries			
\$58,550 to \$63,950 pa	\$69,000 to \$81,000 pa	\$105k to \$125k pa	\$139,650 pa	\$62,300 pa	\$73,100 pa Men	\$70,000 pa Women	\$90,416 pa
Cert IV in Cyber Security	One Year Experience	Cyber Security Analyst	Cyber Security Specialist	First full time job after a TAFE Cert IV	Median University Undergraduate Salary		Median Australian Earnings
NCVER SOS, 2024##	Glassdoor#	SEEK*	Robert Half**	Source: NCVER	Source: QILT, 2023		Source: Grattan Institute, 2025

NCVER data from Student Outcomes Survey in 2024 of Certificate IV in Cyber Security graduates with average error margin applied

[Glassdoor](#) data based on 0 to 1 year experience at 14 October 2024

* [SEEK data](#) based on average Australian Cyber Security Analyst starting salary at 1 May 2025

** [Robert Half](#) data based on starting salary for Melbourne Cyber Security Specialist at 28 May 2025

Analysis

- We ask the TAFE sector to explore options and champion solutions for updating training packages more quickly in the cyber security and IT spaces.
- We encourage the HR and recruitment industries to learn about the benefits of TAFE cyber security and IT credentials and ensure TAFE graduates receive fair remuneration for first roles.
- We call on industry to work even more closely with TAFE to:
 - help augment training packages
 - educate employees about TAFE microcredentials
 - establish TAFE training scholarships for your employees
 - consider TAFE as an applied research partner for solving business critical issues.

Fifteen trends for training, learning and working in cyber security

Through its training delivery research and extensive engagement with cyber security students and industry, Holmesglen's Centre for Cyber Security and Digital Information Technology has identified 15 future trends.

Best Practice Training Trends The 5 emerging techniques for best practice cyber security training.	Student Learning Trends The 5 areas to grow during study that can help cyber security students differentiate themselves.	Graduate Employment Trends The 5 most critical skills and attributes prioritised by employers.
1. Teaching practices will continue to be enhanced alongside technology enhancements. 2. Flexible delivery models will continue to empower students and improve digital literacy. 3. Collaborative platforms like Discord will further improve the efficacy of cyber course delivery. 4. Fast to market microcredential skills sets will help TAFE respond to employer needs. 5. Industry engagement with the training sector will grow as security threats become more complex.	1. Strong and clear resume with links to a portfolio. 2. Strong portfolio that showcases technical skills. 3. Real client experience, such as placement or volunteer projects. 4. Sense of community built through volunteering. 5. Professionalism, well-developed soft skills and strong interpersonal skills.	1. Relevant qualifications and industry certifications to support qualifications (e.g. CompTIA A+, CompTIA Security+, AWS, Cisco, Palo Alto, Fortinet). 2. Technical skills: - pen testing - ethical hacking - cloud engineer - networking fundamentals - programming - knowledge of platforms such as SIEM, next gen firewall, IDS, EDR, etc. 3. Problem solving and analytical skills. 4. Adaptability and willingness to learn. 5. Teamwork and communication skills.

Source: Holmesglen Centre for Cyber Security and Digital Information Technology.

TAFE-based cyber security training is strongly supporting Australian employers to fill critical skills gaps across diverse sectors.

Advances in teaching and delivery

Fast to market microcredential delivery

Holmesglen's cyber security courses deliver industry-focused, hands-on training designed to prepare students for high-demand roles in information technology. The curriculum covers essential skills such as developing and maintaining security policies, identifying and reporting system vulnerabilities, assessing threats to websites and networks, and securing both PC and mobile devices. Holmesglen has also introduced a suite of cyber security microcredentials, supporting individuals and SMEs in upskilling and reskilling to meet Australia's evolving workforce needs. Many of these microcredentials are linked to leading industry certifications, ensuring graduates are job-ready and aligned with employer expectations. Backed by partnerships with Cisco Networking Academy, CompTIA, Fortinet, Palo Alto and Amazon Web Services (AWS), Holmesglen's cyber security programs reflect the latest advances in teaching and delivery, equipping students to respond to the challenges of today's digital landscape.

Simulation excellence

Holmesglen is transforming cyber security and IT education with the launch of its state-of-the-art Cyber Security Operations Centre (CSOC), funded by the Federal Government, at the Chadstone campus. The facility enables remote and on campus students to immerse in a real-world simulated environment, equipping them with the skills required to meet the IT industry's growing demand for skilled cyber security professionals.

The centre provides cyber security professionals at all levels with hands-on, simulation-based education and training. By replicating real-world cyber-attacks and crisis situations, students can practise their skills in a safe, controlled environment. This experiential learning approach sharpens critical thinking, decision-making, and procedural proficiency, ensuring graduates are well-prepared for the complexities of the IT industry.

Inside Holmesglen's Cyber Security Operations Centre (CSOC)

- Red Room for launching simulated real-world attacks
- Blue Room for detection and defence
- Purple Room for communication and collaboration.
- 8 Cisco boards, 35 PCs, 18 x 24" monitors, 55 x 27" monitors
- Dedicated server room



Holmesglen Institute

Holmesglen is a leading Australian provider of vocational training and higher education, and one of Victoria's largest publicly funded TAFEs.

Holmesglen trains approximately 20,000 students across its campuses annually and has more than 160,000 graduates.

Its experience in IT course delivery spans 40 years. In March 2025, Holmesglen opened a \$2 million Cyber Security Operations Centre, funded by the Commonwealth Government, for training Australia's future experts and supporting industry with immersive simulation facilities.



Jamie Weston

Head of Department

Jamie has extensive IT and digital technology expertise and leads Holmesglen Institute's Centre for Cyber Security and Digital Information Technology. He oversees industry-aligned program delivery in cyber security and digital education, working with private and public sector partners to meet national skills needs. In addition to various applied research roles at the Institute, Jamie is the Victorian TAFE ICT Network secretary leading sector-wide initiatives to promote best practice ICT education. He has a Master of Executive Business Administration and a Master of Business and IT from RMIT.

For information, please contact:

T: 03 9209 5210

E: jamie.weston@holmesglen.edu.au

www.holmesglen.edu.au/explore-courses/computing-and-IT

holmesglen.edu.au

© May 2025, Holmesglen Institute.
Information published in this guide was correct at time of printing.
RTO: 0416, IHE: PRV12129, CRICOS Provider Code: 00012G.

B2260525 In Focus Cyber Security Paper A4