Victorian Chamber of Commerce and Industry

Cyber Degree Apprenticeships

Thought Leadership Report

victorianchamber.com.au

Contents

Victorian Chamber of Commerce and Industry

Victorian Chamber of Commerce and Industry | 150 Collins Street, Melbourne VIC 3000 | Phone 03 8662 5333

Foreword

The digital revolution has changed the way we do business.

Employers and employees need to keep up with the constant evolution in digital technologies while they also must protect their online systems and platforms from the ever-increasing threat of cyber-attacks.

This protection requires experienced cyber professionals who can prevent cybercrime with conviction and accuracy. Getting it wrong could have devastating impacts on businesses, causing them to close their doors and leave a trail of jobless employees.

Trust in the business community to handle data safely shatters in the wake of cyber-attacks. The Medibank and Optus data breaches are examples of this. Our economy is also at risk of data loss and ransomware attacks paralysing business operations.

Unfortunately, the demand for advanced cyber professionals has outweighed our local supply of cyber talent. Feedback from industry highlights that recent graduates of traditional university and TAFE cyber security courses are not meeting industry expectations.

Industry needs cyber warriors who have a minimum of three to four years' experience working in cyber roles.

The current certificate, diploma and bachelor models of tertiary training are no longer fit for purpose. Our society needs both head and hand workers – people who can apply critical analysis and problem-solving while implementing practical skills and techniques to resolve issues.

The solution to deliver such a workforce is through enhanced integration between our higher education and vocational education and training (VET) systems. One way to do this is via degree apprenticeships.

A true blend of the two tertiary systems, degree apprenticeships could revolutionise post-high school education. Degree apprentices would earn while they learn, receive on-the-job training and graduate with a degree and industry certifications. Importantly, they would almost be guaranteed a job at the end with their cutting-edge skillset.

One success story is South Australia's first-of-its-kind, five-year degree apprenticeship in software engineering. The University of South Australia program, which is in partnership with BAE Systems and a handful of other industry players, enjoys a "93 per cent retention rate, which is exceptional when you consider that traditional apprenticeships have a 50 per cent retention rate."[1]

These retention rates make a strong case for the formal recognition and establishment of degree apprenticeships across disciplines and all states and territories in Australia.

Education institutions, businesses and governments have the opportunity to evolve alongside the digital revolution and create a new training model that delivers a workforce fit for contemporary societal needs. Now is the time to act and embrace the novel training method of degree apprenticeships, which we lay out in this piece of work.

Why cyber security training needs a rethink

Cyber security is a critical industry worldwide. In Australia, it is projected that nearly **17,000 additional cyber security workers** will be required in both technical and non-technical roles by 2026 to combat the escalating threats of cybercrime.[2]

Why cyber security training needs a rethink

To deliver the 17,000 additional cyber security workers needed, cyber security training models must be fit-for-purpose and able to supply industry with experienced cyber professionals who can capably combat cyber threats.

Currently, there are minimal internship and entry-level cyber security roles in industry. This is because industry has limited capacity and incentives to train newcomers on the job and, therefore, often prefers hiring professionals with at least a few years of experience.

In our recently released Cyber Security and Scams Policy Position,[3] the Victorian Chamber of Commerce and Industry advocated for the adoption of an apprenticeship-style training model for cyber security. This thought leadership report is a deep-dive into that game-changing idea, which could transform cyber training in Australia if implemented correctly with the right policy settings in place.

Taking inspiration from the UK cyber apprenticeships model,[4] the Victorian Chamber believes

"a degree apprenticeship training model for cyber security should be formally recognised, standardised, and trialled across Australia."

The aim is to give aspiring technical cyber professionals the practical work experience they need during their studies to enter the workforce and provide businesses with the technical skills to protect digital systems, devices and data.

There is a desperate need to uplift small and medium business (SMB) cyber security. They form part of supply chains and cyber weaknesses place large organisations and critical infrastructure at risk of an attack as well. *We are only as strong as our weakest link.*

Small businesses account for almost 98 per cent of businesses in Australia, contributing more than $500 billion to our national economy or one-third of our nation's GDP.[5] Ensuring they have access to skilled cyber professionals to keep their businesses operational and free from cyber criminals is essential to Australia's economic prosperity.

1/3 of Australia's GDP.[5]

The Victorian Chamber welcomes the Federal Government's 2023-2030 Australian Cyber Security Strategy, especially its announcement of a new Small Business Cyber Security Resilience Service.[6] However, as this service will be "staffed by professionals who understand small business, cyber security and mental health", it will require cyber professionals with in-depth experience to help business recover from cyber incidents.

Formally recognising and establishing degree apprenticeships in cyber security will help to provide this service with qualified cyber professionals.

Currently, disjointed cyber traineeship models are being trialled, but they are on small scale and primarily benefit large organisations. Australia urgently needs cyber degree apprenticeships so that smaller third-party IT/cyber service providers, who provide IT solutions to the broader SMB community, can access cyber apprentices.

This would benefit cyber students, the education sector and immediate cyber security industry, as well as the broader economy.

Our approach to the report and scope

The Victorian Chamber has employed a mixed-method approach to this thought leadership report. We have engaged in extensive consultation with industry, including education institutions and third-party IT/cyber service providers, to ascertain their views on degree apprenticeships, key challenges to this training model and possible solutions to overcome any barriers.

This was coupled by a comparative analysis of the current cyber security course offerings both locally and internationally. Using the UK cyber apprenticeship model as a basis, the Victorian Chamber has developed our own model that could be implemented in Australia.

Through our consultation with industry, we have identified two broad streams of cyber security roles: technical and consulting. The degree apprenticeship model that we are putting forward is more suited to provide a pipeline of workers for technical cyber roles.

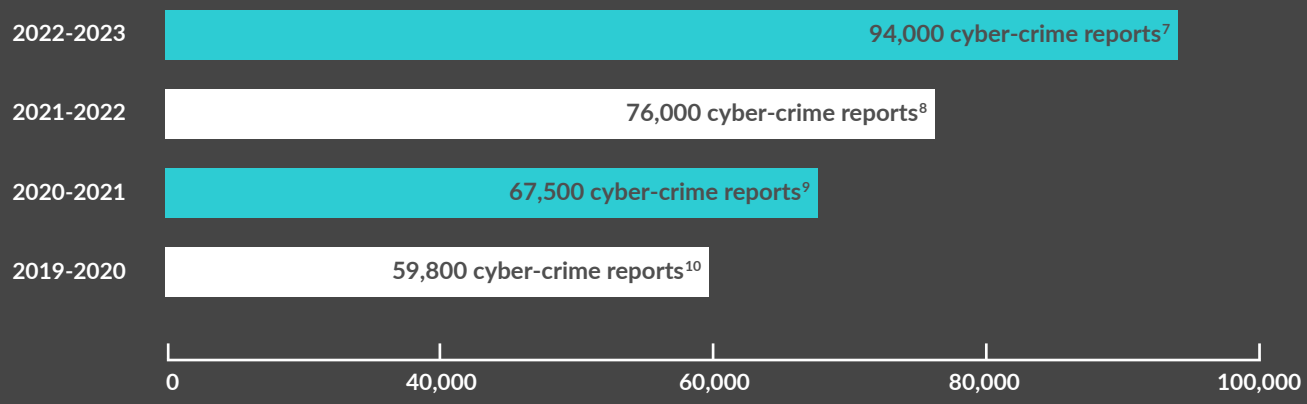
We acknowledge that cyber security consulting and advisory services have multiple entry points and frequently employ staff from a variety of professional backgrounds.

State of cyber in Australia

Cyber weaknesses have a huge impact on the Australian economy.

Cybercrime is on the rise with several notable incidents affecting millions of businesses and consumers alike. The Medibank and Optus breaches are omnipresent in the minds of the millions of Australians impacted by these cyber-attacks.

Across Australia, reports of cybercrimes to the Australian Signals Directorate have surged annually over the last four years:

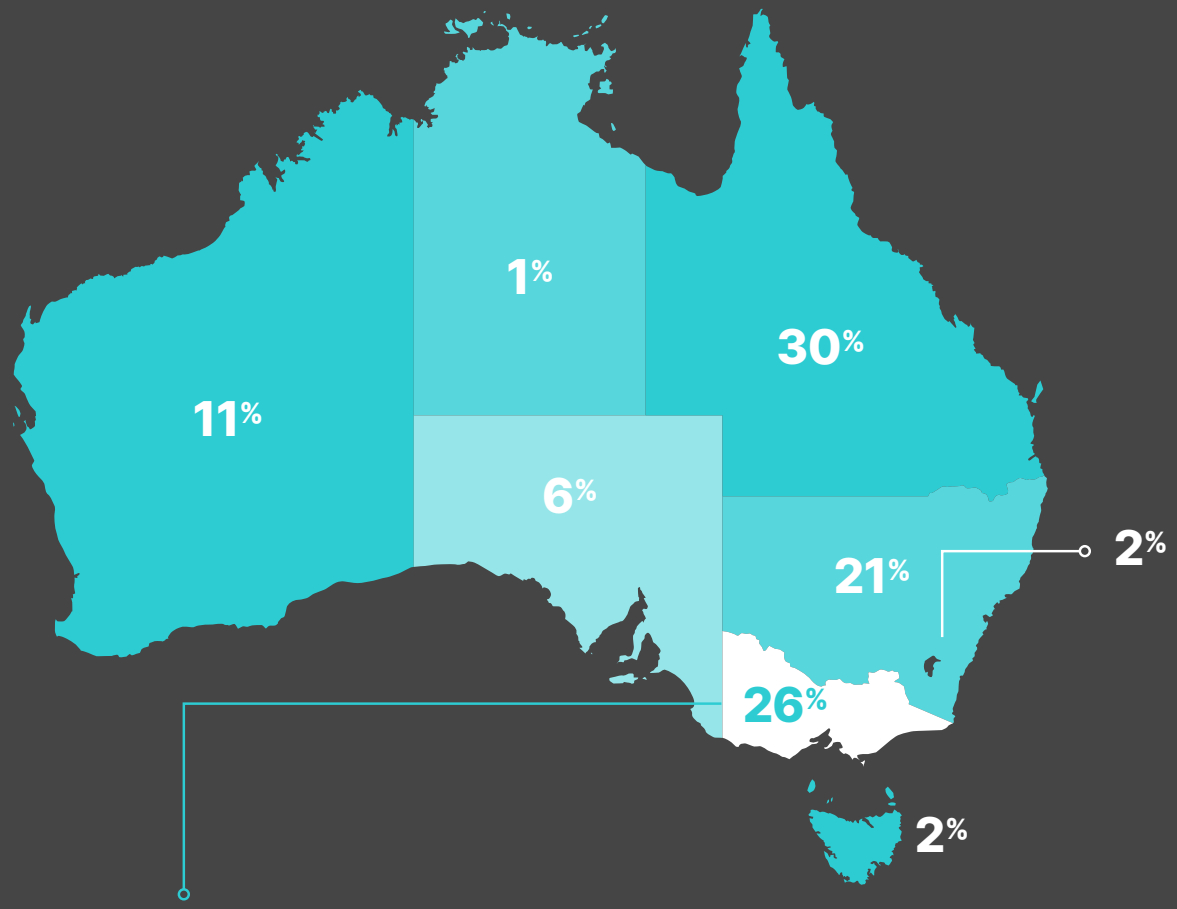


Average losses to cybercrime for businesses according to their size:[11]

	2020-2021	2021-2022	2022-2023
FOR SMALL BUSINESS	$29,901	$39,555	**$45,965**
FOR MEDIUM BUSINESS	$92,400	$88,407	**$97,203**
FOR LARGE BUSINESS	$51,372	$62,233	**$71,598**

Over the last 2 financial years, the average self-reported cost of cybercrime to businesses increased by 14 per cent each year.

Breakdown of cybercrime reports by jurisdiction for FY 2022-23



Victoria has one of the higher reported rates of cybercrime (26 per cent of all cyber-crimes in Australia) relative to population in Australia.[12]

The Australian Cyber Security Centre (ACSC) has found that 48 per cent of SMBs in Australia spend less than AU$500 on their cyber security systems (risk assessments, firewalls, and infrastructure) per year.[13] Concerningly, almost half of SMBs rated their knowledge of cyber security systems as average or below average.[14] With SMBs making up the large majority of Australia's business community, we must safeguard this vital part of our economy.

To fend off these cyber threats, ensuring Australia has a highly skilled cyber workforce must be at the forefront of government policy.

Shortfalls of the current cyber security training model

There are many challenges facing the existing training system when producing experienced cyber professionals that are job-ready immediately upon completion of their studies.

Lack of formal recognition of degree apprenticeships

Australia has yet to formally recognise and facilitate degree apprenticeships. In Victoria, it is understood that degree apprenticeships are not endorsed under the Education and Training Act 2006. To get around this, degree apprenticeship models have been rolled out in a combination of traineeships in the first year and then transition into bachelor's degrees for the second and third years.

Lack of incentives for businesses to take on apprentices

Under the current traineeship/bachelor's degree model, businesses are not eligible to receive government incentives to take on degree apprentices as they do not fit within the traditional apprenticeship model. Therefore, industry engagement in and knowledge of degree apprenticeships is minimal due to the barriers of time and cost associated with taking on untrained staff.

Additional barriers to access cyber staff for small and medium businesses

One of the main issues with the current traineeship and academy programs is that they primarily service the cyber problems at large organisations. There are limited programs in place that provide a pipeline of new cyber talent to small third-party IT/cyber service providers, that usually protect small, medium and family businesses from cyber threats.

Lack of career pathway

In the Free TAFE system in Victoria, there is no pathway to continue studies in cyber security following the Certificate IV in Cyber Security. The Certificate IV does not provide students with the in-depth knowledge and skills required for entry-level roles in cyber security.

Rapidly changing technology

The technologies and techniques used in the cyber industry are constantly evolving. The content taught in undergraduate courses can be outdated by the time students finish their studies.

Lack of real-world industry experience

Many aspiring cyber professionals lack practical skills because they have limited work experience opportunities in industry, which makes it difficult for them to break into the industry.

Shortfalls of the current cyber security training model

Lack of 'head' and 'hand' workers

TAFE institutions focus heavily on development of hands-on skills, while university courses are known to be theory-heavy. Graduates from tertiary education programs, therefore, tend to not have both practical and theoretical backgrounds. Our economy needs workers with both extensive knowledge and practical skills.

Limited entry-level cyber roles

When hiring, industry looks for cyber professionals that have demonstrated experience in industry, as well as the technical and soft skills required to secure digital environments and daily operations. Currently, there are limited entry-level cyber security roles in industry. Eighty-seven per cent of cyber security jobs require more than three years of work experience.[15] Yet, industry desperately needs more experienced workers who are ready to fight cyber criminals upon graduation.

Lack of time and resources to train apprentices on the job

One of the greatest challenges businesses face when training newcomers to the cyber industry is a lack of time. Graduates, interns and apprentices all require in-house coaching, mentoring and education, which businesses are rarely in a position to provide.

Retention of cyber security professionals

Given the strong need for cyber security professionals across our economy, cyber professionals are often headhunted. Retention of cyber professionals is challenging for employers who help train them.

Absence of industry certifications in undergraduate courses

Industry certifications for cyber security (e.g., SANS, CompTIA+ certifications) are rarely incorporated into training programs. Some employers look for these certifications when hiring new cyber professionals. These certifications can range in cost from under AU$500 to more than AU$10,000. In most cases these qualifications are not attainable for students independently and are sponsored by companies when training up new staff.

Lack of a standard curriculum

At present, there is no standard curriculum for cyber security courses, neither is there a professional body or registry that oversees training and development in the field. As such, the quality of cyber security courses can vary greatly. Setting a standard national curriculum would ensure tertiary courses deliver the skills and training that meet industry expectations.

Solutions to improve cyber security training

Australia must rethink its approach to training cyber security professionals to address the many shortfalls in the current training system.

Incentives for industry to take on apprentices

Industry needs to be rewarded for helping train the next generation of cyber professionals. Incentives could include tax breaks, wrap-around support services that set up both employers and apprentices for successful completion of apprenticeships (e.g., Apprenticeship Support Australia (ASA)), access to further education and training for all staff at reduced prices, educators in industry to assist with training and implementing staff retention policies.

Formal recognition of degree apprenticeships

The Federal Government must take the lead on formally recognising and establishing degree apprenticeships in Australia. By doing so, businesses will have greater incentives to participate in degree apprenticeship programs through access to hiring incentives and wage subsidies.

Government support is key for building the momentum needed to deliver large skills needs. The formal recognition of degree apprenticeships is aimed at providing a more streamlined training pathway for all parties involved – aspiring professionals, businesses and education institutions. The current traineeship/bachelor degree model works and should continue as needed by industry, but can be complex for parties to navigate.

For traditional apprenticeships, hiring incentives are available to eligible employers and consists of two one-off payments made after six and 12 months of employing an apprentice.[16] The Victorian Chamber advocates for an additional hiring incentive for businesses that is made upon successful completion of apprenticeships.[17] This would also help to raise completion rates.

The Federal Government must take the lead on formally recognising and establishing degree apprenticeships in Australia.

Solutions to improve cyber security training

Guaranteeing greater return on investment for industry

Small and medium businesses can be hesitant to take on apprentices as they risk investing a lot of time and resources into training them only to have apprentices leave immediately upon completion of their studies. To incentivise participation from more businesses in cyber apprenticeship programs, retention policies should be explored to guarantee greater return on investment.

Better integration between the university and VET systems

Students need to receive more robust theoretical training in the classroom, complemented by hands-on, practical work experience. Developing a tertiary system that has both in-depth theoretical and practical components is key to meet the demands of our modern economy. Permeability and interoperability of the two systems is central to achieving this.

Partnerships with industry

Education providers that form partnerships with industry are key to creating more job-ready graduates. For example, Microsoft has formed partnerships with TAFE institutions in Australia to enhance the existing IT curriculum by providing students with the chance to work in large-scale IT environments, such as hyperscale cloud datacentres.[18] While the curriculum may slightly differ across institutions, the primary objective remains consistent: to create more job opportunities for aspiring cyber professionals whose task is to protect the nation from the increasing threat of cyber-attacks.

Three-month bootcamp

A bootcamp at the beginning of degree apprenticeships would introduce students to general information technology concepts. Running intensive classes over a period of three months would ensure students have a baseline understanding of information technology and cyber security before students proceed to on-the-job training in industry.

Staggered time in industry

During their first year of study, students are to spend more time at university studying (one to two days on the job training and three to four days studying coursework). As time goes on, this split will gradually shift to focus more on practical, hands-on learning (three to four days of on-the-job training and one to two days studying).

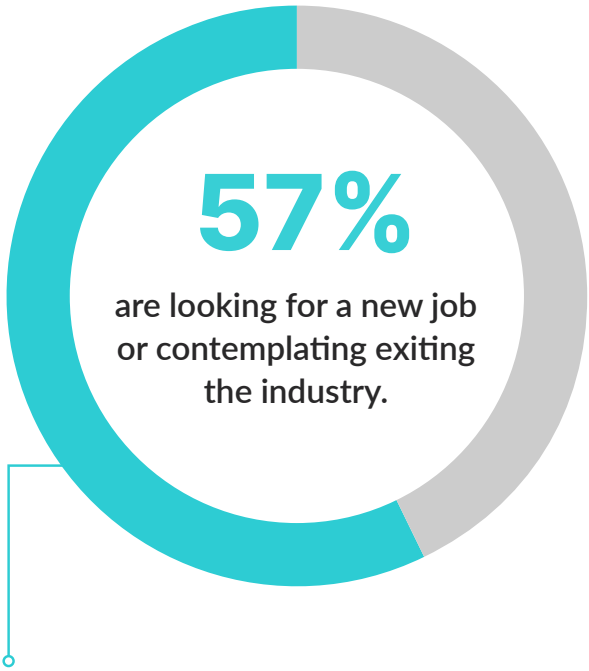
Entry-level roles

Students could start in an entry-level service desk role and transition into a cyber security position. Specific guidelines need to be put in place to ensure students can learn basic tasks on the job, while providing valuable input into business operations. Tasks assigned to students also need to be related to their level of study. These will need to be standardised in cyber degree apprenticeships.

Educators in industry

Experienced and qualified educators in industry to help train degree apprentices would alleviate some of the pressures from employers who often have limited education training themselves to teach others well. Like educators in the allied health industry, cyber educators would be qualified cyber professionals themselves with a minimum of ten years' experience in IT and five years' experience in cyber security. They would be affiliated with an education provider and have undergone training that equips them with the skills to educate others. Educators could rotate between multiple businesses, providing valuable support to both employers and apprentices.

Government funding allocated to the Cyber Wardens[19] program could be repurposed to train experienced cyber educators in industry. Or, given that uplifting cyber security is in Australia's national interest, national security funding from REDSPICE[20] could also be leveraged.



Pivoting burnt-out cyber professionals towards becoming educators

A recent study revealed that 57 per cent of local cyber security professionals in Australia and New Zealand are either looking for a new job or contemplating exiting the cyber industry entirely.[21]

The average tenure of Chief Information Security Officers (CISOs) is just over two years, due to high stress and burnout.[22] With burnout rife in the industry, taking a step out of the hotseat and into an educator role might be an appealing career move for those needing to decompress.

Directing burnt-out cyber professionals down the educator path would overcome the challenge of finding experienced cyber professionals that have the industry competency to become an educator.

Industry certifications in tertiary curriculum

For technical cyber security roles, businesses frequently value and look for new grads that hold industry certifications (e.g., SANS, CompTIA Security+, GIAC Information Security Fundamentals). Embedding industry certification into existing courses would require modifying the curriculum, ensuring teachers are familiar with the content and incorporating any costs associated with attaining the industry certifications into HESC-HELP debt schemes.

Cyber security course curriculum standardisation

Clear metrics, theory and a baseline of technical and soft skills must be set to ensure all cyber security students meet a minimum level of training and instil confidence in industry when hiring cyber apprentices and new grads.

Professional register of cyber security professionals

The standardisation of course curriculum should be accompanied by a professional registry of chartered cyber professionals – much like in the medical industry with registered nurses and doctors. Other countries around the world, most notably the UK,[23] have professional registrations for cyber security professionals. Australia must follow suit if it wants to create a credible cyber industry.

Soft skills

Soft skills are an integral part of all roles, including cyber security. The cyber industry favours new graduates who demonstrate strong communication skills, stakeholder engagement, curiosity, initiative and self-motivation. These skills are important when communicating how IT and cyber technologies translate into business propositions.

Australian Cyber Degree Apprenticeships

Australia is in need of improved ways to create a pipeline of skilled technical cyber professionals, one that uplifts the cyber security of all businesses – small, medium and large.

The Victorian Chamber has developed the below Cyber Degree Apprenticeship model, which is based on the UK cyber apprenticeships model,[24] and aimed at equipping industry with experienced cyber professionals. It incorporates some of the suggested improvements mentioned above.

1st YEAR

Diploma – Semester 1

3-MONTH BOOTCAMP

full-time in classrooom

Diploma – Semester 2

2 days in industry
3 days in classroom

6-MONTH MARK

ROLES:

- ✓ First Level IT Support

2nd YEAR

Bachelor's Degree

3 days in industry
2 days in classroom

12-MONTH MARK

ROLES:

- ✓ Cyber Security Analyst
- ✓ Forensics and Incident Response Analyst
- ✓ Threat Intelligence
- ✓ Security Operations Centre (SOC) Analyst
- ✓ Penetration Tester
- ✓ SecDevOps

1 2

Educators in industry | Hiring incentive for employers | Industry certifications

3rd YEAR
Bachelor's Degree

3 days in industry
2 days in classroom

UPON SUCCESSFUL COMPLETION

ROLES:

- ✓ Cyber Security Analyst
- ✓ Forensics and Incident Response Analyst
- ✓ Threat Intelligence
- ✓ Security Operations Centre (SOC) Analyst
- ✓ Penetration Tester
- ✓ SecDevOps
- ✓ Cloud Anayst

3

MASTER'S DEGREE
1st Year

4 days in industry
1 day in classroom

ROLES:

- ✓ Cyber Risk Manager
- ✓ Cyber Incident Manager
- ✓ Cyber Security Engineer

2nd Year

4 days in industry
1 day in classroom

ROLES:

- ✓ Cyber Risk Manager
- ✓ Cyber Incident Manager
- ✓ Cyber Security Engineer

4 & 5

Although we are advocating for the formal recognition and standardisation of degree apprenticeships as a qualification in their own right, we acknowledge that this will take some time and, in the interim, should proceed with the diploma/degree model.

Cyber degree apprenticeships would combine practical work experience in industry with theoretical learning, enhancing collaboration between businesses and the education sector, providing a structured training model that is easy for learners and employers to navigate.

Cyber degree apprenticeships would help facilitate a pipeline of skilled workers entering the cyber workforce. They could service government initiatives such as the proposed Small Business Cyber Resilience Service.[25]

Successful recruitment

Similar to traditional apprenticeships, cyber degree apprentices could find their own employer to undertake a degree apprenticeship. Once both apprentices and employers are ready to proceed with a formal apprenticeship agreement, a Group Training Organisation (GTO) validates their agreement by providing a legal contract of employment confirming that the organisation and apprentice are in an apprenticeship. From here, the GTO provides support for the organisation on how to deliver adequate on-the-job training.

Alternatively, businesses could register their interest and availability to take on degree apprentices, as well as the type of cyber roles on offer in their organisation, via the Apprenticeship Support Australia (ASA) network.

Greater attention is needed on matching candidates with roles that are suited to them, their strengths and interests. The Victorian Chamber advocates for an increased focus on career services, which help individuals to identify their professional strengths and align them with suitable career opportunities.[26] A dedicated focus on robust career guidance would see more people with the right interests and attributes into the cyber industry and greater staff retention rates.

The Cyber Academy,[27] in partnership with Deloitte, Swinburne University of Technology, TAFE NSW, and the University of Wollongong, has developed a human capability framework to recruit aspiring cyber professionals to the program based on their aptitude, attitude and talent. From this, the Academy can determine which cyber roles applicants will be best suited to.

A formalised Australian Cyber Degree Apprenticeship model should take inspiration from this innovative recruitment method and target both local and international aspiring cyber professionals. A cyber degree apprenticeship program should have the same eligibility criteria as traditional apprenticeships, and not impose additional requirements such as to restrict internationally born Australians.

Industry certifications

Industry certifications in cyber security are a way for individuals to demonstrate sound technical skills in areas of specialisation. There are hundreds of different industry certifications that vary based on the software systems and specialisation stream:

- **Red Team/Attackers:** discovering vulnerabilities in cyber security systems.[28]
- **Blue Team/Defenders:** protecting security systems.[29]
- **Managers:** managing teams and applying security controls.[30]

Industry certifications are frequently sought after by employers looking for technical cyber specialists. However, for employers seeking to hire cyber professionals in governance, risk and compliance roles, industry certifications are less of a prerequisite.

There are a few barriers to attaining industry certifications. The costs associated with acquiring them can range from AU$400 (e.g., CompTIA Security+), to more than AU$10,000 (e.g., SANS cyber security courses). The high cost of these certifications makes them inaccessible to many.

Student loans (e.g., HELP-HECS debt scheme) are key to incentivising more cyber professionals to attain industry certifications.

Below is a list of some of the industry certifications that could be incorporated into an Australia degree apprenticeship model for cyber security.

Blue Team/Defenders

Amazon Web Services (AWS): Certified Cloud Practitioner (AWS-CP)

A beginner-level defender/blue team certification that validates an individual's ability to effectively perform security architecture and engineering on an AWS platform. To attain this certification, students must demonstrate confident knowledge of security concepts in relation to the AWS software systems. As this is a beginner certification, there are no prerequisites.

AWS is a system that is widely used across the public sector and education industry.[31] Some of its notable clients include the University of Auckland, University of Newcastle, and Australian Bureau of Statistics.[32]

Microsoft: Azure Fundamentals (AZ-900)

A beginner-level certification that validates the technical ability of individuals to use Microsoft Azure to deliver secure cloud services. It is under the technical domain of security architecture and engineering. This certificate tests the participant's knowledge of Azure, a cloud service used by more than 400,000 businesses internationally including Coca-Cola, Bing and CyberCX. Microsoft recommends that candidates have some level of basic knowledge in an area of IT before attempting to attain this certification, however this is not mandatory.[33]

Microsoft: Azure Security Engineer Associate

An intermediate-level defender/blue team certification in security architecture and engineering. Candidates for this program are expected to have some level of practical experience in the administration of Microsoft Azure and hybrid environments, as well as a solid understanding of networking, computing and storage concepts in Azure. This certification validates important skills needed to implement security functions in an Azure environment.[34]

Red Team/Attackers

TCM: Practical Network Penetration Tester

A beginner-level ethical hacking certification. Students have five days to complete a written assessment and two days to finish a written professional report, which they present to a team of assessors. Relevant study resources are also included to sit the exam.[35] There are no prerequisites for this certification.

CompTIA Pen Testing+

A beginner to intermediate-level penetration testing certification that aims to certify the ability of a cyber security professional to test an online system for vulnerabilities and manage risks. This certification focuses mainly on penetration testing for cloud-based applications. Attainers of this certification must demonstrate a proven ability to plan, scope and test for weaknesses in digital environments.[36]

GIAC Penetration Tester

An advanced penetration testing certification that aims to extend the ability of experienced security professionals to perform penetration testing and administer risk management methodologies. While there is no explicit requirement that the participant has a certain amount of experience in the area, the course requires advanced working technical knowledge of networking and operating systems concepts. This certification requires specialised training that can be acquired through SANs, a specialised training provider. These courses, however, typically come with a very high price tag and must be renewed periodically.[37]

Managers

Risk manager certifications aim to equip candidates with a generalist level understanding of a range of cyber security risk assessment and management principles. Certifications in this area include:

- **CompTIA: Security+**
- **ISC2: Systems Security Certified Practitioner (SSCP)**
- **GIAC: Security Essentials (GSEC)**

Attainment of a certificate in this area validates the baseline technical skills and knowledge an individual needs to manage complex cyber environments and risks. One specific certification at the managerial level is:

GIAC Strategic Planning, Policy, and Leadership (GSTRT)

A certification catered to experienced professionals looking to upskill into a management position. The GSTRT certification is tailored to individuals who are in or aspire to be in leadership roles such as Chief Information Security Officers (CISOs), Information Security Officers, Security Directors and Security Managers. Those who hold this certification are expected to be able to strategically apply cyber security and risk management principles to lead organisations.[38]

The inclusion of some of these certifications into undergraduate cyber security training, such as degree apprenticeships, would help to make the next generation of cyber professionals more employable upon completion of their studies.

Funding mechanism

Cyber degree apprenticeships should be covered by the Federal HECS-HELP[39] debt initiative for local students to receive a commonwealth-supported place, or similar arrangement. This should cover all costs associated with cyber degree apprenticeships, including industry certifications.

International students wishing to partake in this program would pay a full-fee price.

Further, to enhance completion rates, the costs of any cyber security courses that fall within the Free TAFE system should be placed on HECS-HELP debt schemes and only wiped upon successful completion.

Challenges with cyber degree apprenticeships

Implementing cyber degree apprenticeships comes with its own set of challenges. Some of the greatest barriers relate to formal recognition of degree apprenticeships, modifications to the Australia Qualifications Framework and overcoming industrial relations challenges as well as certain structural barriers.

Getting Government onboard

The Federal Government has the opportunity to take the lead on necessary reform to enhance integration between the higher education and VET systems in Australia – a key component of the Australian Universities Accord. And what better place to start than formally recognising, standardising and establishing degree apprenticeships across the nation.

Government backing of degree apprenticeships is essential for their wide uptake in society. Bold policy reform and commitment by Government now can revitalise the entire tertiary education system, making it more fit-for-purpose and up to date with the latest industry trends.

Degree apprenticeships in this model should include a national training contract. The qualification then needs to be endorsed in each state by the State Training Authority and approved to be delivered through an apprenticeship model. In Victoria, the Education and Training Reform Act 2006 may need to be modified to endorse degree apprenticeships at the state level.

Further, promotion of degree apprenticeships as a credible study pathway right across metropolitan and regional Australia must be at the forefront of government agenda. Aspiring professionals and businesses alike need to be made unaware of degree apprenticeships as a training option. Business chambers of commerce are well-placed to deliver awareness raising campaigns and information sessions on degree apprenticeships to their vast networks of small, medium and large enterprises.

Modifying the Australian Qualifications Framework (AQF)

Proposing a new training package or modifying an existing one to reflect current trends in industry is by no means an easy task. Approval of a training package is a lengthy three-to-five-year process, which requires Australian education regulators to identify how industry demand can be broken down into different achievable core skills, as well as consideration of the most suitable teaching method.

To administer degree apprenticeships alongside traditional university bachelor's and master's degrees, the AQF Level 7 (bachelor's degree qualification type) and AQF Level 9 (master's degree qualification type) would need to recognise on-the-job training.

Despite the rigorousness of this task, the recognition of on-the-job training in the high education system should be front and centre of policy reform.

Industry involvement in cyber training

Entry-level roles for early-career cyber security professionals are uncommon. The combination of time commitment required to train up new technical cyber staff and lack of existing experienced cyber professionals to assist and supervise can make it challenging for organisations to take on new graduates.

Businesses look for cyber professionals with a proven record to secure their systems. Data collected for cyber security job advertisements shows that only 13 per cent of cyber security roles seek individuals with less than two years of experience and 33 per cent of jobs require applicants to have more than eight years of experience.[40]

With demand for experienced cyber security professionals forecasted to continually rise, entry-level opportunities in industry are vital to Australia's cyber security maturity. Cyber degree apprenticeships would provide a pathway for aspiring cyber professionals to enter the workforce.

For an apprenticeship-style training model to work, industry needs to step up. The Australian business community must foster a culture of on-the-job training, like in many European countries. Germany and Switzerland stand out as leaders in this space.[41]

Research into the return on investment for apprenticeships shows that ROI increases over time.[42] This aligns with apprentices gaining more skills and productivity as their experience accrues. To reap the advantages of retaining apprentices upon completion of their studies, some large organisations offer apprentices sign-on bonuses on top of their salary.

More robust on-the-job training in industry is necessary for Australia to build an army of cyber warriors ready to defend our mum-and-dad businesses, local supply chains, critical infrastructure, and national sovereignty from the escalating number of cyber threats.

Case Study: Cyber Academy

Australia's cyber workforce is projected to have significant shortfalls when delivering the security needs of the country into the future. Evidently, the current method of attracting, educating and retaining a diverse and resilient cyber workforce is not fit for purpose.

In response to this, Swinburne University of Technology, University of Wollongong, TAFE NSW, and Deloitte developed their Cyber Academy with support from the NSW Department of Education. Designed to help narrow the projected workforce shortages in the sector, the Cyber Academy seeks to remove structural barriers, creating a diverse workforce and new pathways into the cyber industry.

Students enrol in a three-year work integrated learning (WiL) degree apprentice program where they also complete a diploma. In this 'earn while you learn' model, students work three days a week in industry and spend the other two days a week studying at their associated education institution. For students enrolled at Swinburne University of Technology, at the end of three years they will graduate with a Diploma of IT Advanced Networking and Cyber Security as well as a Bachelor of Cyber Security.

For the WiL component of the program, students can be placed across different public and private sector organisations and receive a salary of $40,000 pro rata.

In addition to attaining a Bachelor and Diploma, students also have the opportunity to obtain numerous professional certifications both through their study and work placements, which are critical for developing their skills and differentiating themselves in the labour market.

After successfully completing its pilot phase, the Cyber Academy is currently onboarding its second cohort of students, with the first cohort entering their second year of the program.

Various organisations have supported the program by taking on Cyber Academy students including Coles, Linfox, AGL, and more. Coles noted that their cyber students were really "hitting the mark" and fundamentally "great contributors for their level". AGL commented that they were "extremely happy with the program" and "see it as an annual stream to bring in future cyber talent".

Swinburne University of Technology has also noticed that Cyber Academy students are exceptionally engaged in their learning activities and classes.

External organisations to the Cyber Academy are also recognising the cyber students' burgeoning success. Noor Zafar in NSW was selected to be on CISCO's all female 'Dream Team' protecting the entire communications systems of the Women's World Cup in 2023[43] and Ben Riles in Victoria was nominated for the Australian Information Security Association's Tertiary Student of the Year Award.

This Cyber Academy, similar to our proposed degree apprenticeship model, has proved successful in its first intake of students. However, to increase industry engagement in such programs, businesses need to know that degree apprenticeship models exist and they require support to get involved.

Apprenticeship Support Australia

Intermediary support services between employers and apprentices are crucial to successful apprenticeship completions. Training up the future generation of workers can be a time-consuming process for busy employers. Support networks need to be in place and available to the pipeline of cyber talent to ensure that businesses and apprentices are set up for success.

Industry has highlighted the need for assistance with navigating the complex regulatory landscape associated with taking on apprentices. Services such as Apprenticeships Support Australia (ASA)[44] play an essential role in providing skills development advice and solutions to businesses across Australia and deliver a significantly higher apprentice completion rate than the national average.

ASA will need to be expanded to include degree apprenticeships. This would help to streamline the process of finding and onboarding degree apprentices in industry and, importantly, ensure the successful completion of degree apprenticeships.

Overcoming industrial relations barriers

One key barrier to industry engagement in apprenticeships, in general, is the full-time pay requirement even when apprentices are spending several hours per week completing their tertiary studies.

Degree apprenticeships, which require more in-depth theoretical study at education institutions, should favour flexibility in their training arrangements. In such a system, degree apprentices would be paid for hours worked and accrue leave, similar to part-time employees. In our proposed model, this would initially be two days per week progressing to three days per week.

Consideration should also be given to different pay scales based on varying levels of apprenticeships. Pay scales should be based on level of experience and roles in industry. The progression of cyber degree apprentices to more advanced roles in industry should be reflected in their salaries.

Modifying the award would be more attractive to employers and increase the number of businesses engaging in cyber degree apprenticeships.

Breaking down structural barriers

There are many structural barriers impeding entry into Australia's cyber industry. Increasing diversity in cyber security is a primary challenge for the industry.

Cyber is historically a male-dominated industry across Australia. Women only represent 26 per cent of the cyber workforce and, in Victoria, this statistic is even more bleak with women making up just 22 per cent of the workforce.[45] Getting more women into cyber must be front of mind for policy makers if Australia is to reach forecast workforce targets.

Mentorship is one way to promote diversity in the cyber industry. Initiatives such as Australian Women in Security Network (AWSN) and the BUSY sisters mentoring program[46] could be expanded and incorporated into cyber degree apprenticeships and help address the gender imbalance.

Careful consideration needs to be given to the types of cyber roles suited for women. According to the Tech Council of Australia, women are more likely to come into the tech industry later in life and, therefore, at a time when they have more financial commitments. This is one reason why entry-level roles are less appealing to women entering the cyber industry. An education system that pays people for their time to learn – the *earn while you learn* model – is better for women and, if widely adopted, would supercharge female participation in cyber.

Dedicated assistance to improve the training and career pathways for Indigenous Australians, people with disability and neurodiverse individuals into the cyber industry should also be a key focus of policy reform. Inspiration can be taken from platforms such as Genius Armoury,[47] which identifies an untapped pool of talent from the autistic community and attracts them to the cyber industry. These diverse cohorts can help tackle the critical skills shortage.

Non-Australian citizens seeking to work in cyber also struggle to enter the industry. They are frequently blocked when attempting to obtain security clearances, particularly in government departments and agencies. This places further restraints on the pool of cyber talent that Australian businesses can tap into. Reviewing rigid security clearances for low-risk functions would enable more internationally born individuals to gain work experience whilst they study and help service our local cyber security ecosystem.

Background

Comparative analysis of current course offerings

Today, there are several different avenues to enter the cyber security industry. Universities offer bachelor's and master's degrees, TAFEs and dual-sector universities offer certificates and diplomas, and there are also short courses and micro-credentials aimed at rapid reskilling and upskilling of the workforce.

Whilst tertiary-level training programs equip students with a thorough theoretical understanding of cyber security,[48] they can lack practical, hands-on experience, making it hard for students to enter the workforce.

This section provides a comparative analysis of the current course offerings for cyber security both locally and internationally. It identifies strengthens and weaknesses of each course and considers how a degree apprenticeship model could address these.

Australian tertiary training in cyber security

This section focuses on highlighting practical work experience and placements in industry, which lead to improved employability of graduates. The objective is to ascertain the standard practical work experience currently offered to students and how this can be enhanced in a degree apprenticeship training model.

Universities

Monash University and Deakin University both deliver a Bachelor of Information Technology with a major in cyber security. These degrees can be attained within three years of full-time study. Classes are taught through a combination of practical classes and lectures. This helps students to build a portfolio of projects while learning relevant theory. All the degrees are accredited by the Australian Computer Society.

Monash University dedicates approximately half of its undergraduate degree's final year to either a capstone project or a 22-week part-time internship. Internship opportunities are only available to students achieving a weighted average mark (WAM) of 65 per cent and above.[49]

Deakin University offers a range of options to give students industry experience. There is the self-sourced paid professional practice option where students can receive credit for 450 to 950 hours of related work experience.[50] Students can also choose from either a capstone unit, where they deliver a real-life project for a client,[51] or a shorter version of the professional practice unit that has an unpaid option.[52]

To complete a cyber security degree at The University of Melbourne, students must undertake the Bachelor of Science or Bachelor of Design specialising in an IT-related stream (e.g., computational science).[53] After this, students can major in cyber security at the master's level. Completion of these two qualifications takes five years.

The University of Melbourne offers a capstone project at the undergraduate level and 12-week internships to students at the master's level.[54] For students wishing to participate in an internship in their bachelor's degree, an 80-to-100-hour internship elective can be taken. The University of Melbourne also offers other initiatives such as the students@work program[55] with the aim of providing students with industry exposure.

Overall, the practical work experience in industry in these undergraduate and master's courses is short-term – either via capstone project or part-time internship. Students would benefit from longer, full-time appointments in industry to fine tune their practical and soft skills.

Dual sector institutions

Dual sector institutions, which are accredited to deliver VET and university-level courses, have a mix of undergraduate degrees, diplomas, and certificates in cyber security.

RMIT University offers a Bachelor of Cyber Security, based on the Australian Signals Directorate's framework for skills needed to combat cyber threats. RMIT also offers a Bachelor of Information Technology and Bachelor of Computer Science with a major in cyber security. All above degrees can be completed in three years.

RMIT has designed its courses with the aim of giving students hands-on experience before graduation. After completing the three-year program, students that meet the selection criteria have the option to be placed in a university-sourced internship with an industry partner over an optional fourth year. Alternatively, students can complete a capstone project during their three-year undergraduate program.

In Victoria, VCE students achieving a study score above 86 ATAR points can directly enter the Bachelor of Information Technology or Bachelor of Computer Science (professional), which includes the 4th Year industry placement.[56]

RMIT University also offers a Certificate IV in Cyber Security, which is free for domestic students under the Free TAFE initiative.[57] This is a short course that aims to help early career professionals enter the cyber security industry.[58]

Victoria University delivers a Bachelor of Information Technology with a major in cyber security. It provides students the opportunity to participate in a final year capstone project, where they deliver a project to a real client.

Federation University delivers their four-year Bachelor of IT (Professional Practice) through a co-operative educational model. In partnership with IBM and Kyndryl, 1600-hour paid internships are incorporated in the final two years of the undergraduate degree.[59] IBM Australia benefits from being able to access a consistent pipeline of talent, while Federation University has seen a 30 per cent increase in graduate employability. IBM's continuous investment into developing hands-on skills and mentoring has also resulted in the average graduation mark from the degree being a Distinction.[60]

Federation University has also partnered with 300 high schools across Australia to deliver programs targeted at middle school students. One such initiative is the Pathways in Technology Early College High School (P-TECH) program, a six-week paid internship program where participants receive a Certificate III in Information Technology upon completion.[61]

Swinburne University's Cyber Academy, delivered in partnership with Deloitte, is also a notable instance of an industry-focused tertiary program. Over three years, students complete a diploma and bachelor's degree in cyber security.[62] Students spend three days per week doing paid work in industry and two days per week studying at Swinburne. Upon completion, students are equipped with industry experience, a relevant degree and better access to entry-level job opportunities in industry. Due to capacity limitations, entry into this program is highly competitive.

The more co–operative educational model employed by Federation University and Swinburne University are a step in the right direction, giving graduates paid, hands-on experience in industry partner organisations during their studies. This should be standardised across all cyber security training courses.

TAFEs

TAFE institutions across Australia have partnered with government to deliver key programs in response to the cyber skill shortage. Initiatives like TAFEcyber bring together TAFEs and dual sector universities to provide training and upskilling for those wishing to pursue a career in cyber.

In Victoria, partner institutions of TAFEcyber include Box Hill Institute, Melbourne Polytechnic and Victoria University.[63] Joining the TAFEcyber consortium as a member requires a joining fee of AU$15,000 initially and then AU$10,000 per annum. The few education providers that participate in the TAFEcyber initiative in Victoria suggests the costs act as a barrier to participation.

In Victoria, Free TAFE[64] was designed to incentivise more students to pursue a career in a trade. Currently, this initiative covers the Certificate IV in Cyber Security. More advanced qualifications such as Diplomas or Advanced Diplomas in Cyber Security are excluded from Free TAFE, leading to low enrolments in these courses.

The exclusion of these qualifications from Free TAFE means that there is no pathway forward in the Free TAFE system to pursue further studies in cyber security upon completion of a Certificate IV. The Certificate IV is also an entry-level program designed to introduce cyber security concepts, meaning that many graduates of this certificate are not adequately prepared even for entry-level technical roles.

A further limitation to the Free TAFE system is its high attrition rates. Tertiary education providers need to find other ways to incentivise completion. One successful program is the Victorian Government's Digital Jobs program,[65] whereby participants complete a free 12-week training course in a digital skills stream of their choice before applying for a 12-week placement in industry. Feedback from industry has indicated that a paid industry placement at the end of the program encourages completion.

At Box Hill Institute, they offer a Certificate IV of Cyber Security. Over the course of one year, students gain an introductory understanding of cyber security concepts. This course also acts as a pathway for students to study the Bachelor of Information Technology at the Institute.[66]

Short courses

Short courses are becoming more common for professionals looking to break into a cyber security-related career. Victoria University Polytechnic administers the short course THABC Cybersecurity Essentials. The program is based on the CISCO network academy 'Cyber Security Essentials' modules. Running intensively over a four-week period through a combination of eight self-paced learning and seminars, this short course is targeted towards mid-career workers wishing to transition careers into cyber.[67]

Another short course is the Essential Eight Assessment Course developed by the Australian Signals Directorate. This course requires participants to have four years of experience in a technical ICT role, a Certificate IV qualification in a technical ICT discipline, and Australian Citizenship.[68] The TAFEcyber consortium delivers this program. As it stands, entry requirements for this course bar most mid-career individuals and those looking to transition from a non-cyber-related background.

Graduate programs and training centres

Graduate programs aim to further technical and soft skills of new graduates. Host organisations hire graduates into entry-level roles and provide structured on-the-job training and mentoring.

EY is a firm that offers one such program with a focus on cyber security consultancy. In their first 12 months, graduates rotate through a series of different roles under the guidance of a mentor.[69] This program exposes graduates to projects that early-career professionals usually do not have access to, with the aim of fast-tracking their career development. EY's graduate program is highly selective and only takes on a small number of participants.

The CyberCX Academy is another fast-tracked, six-month program, whereby aspiring cyber security professionals (associates) are trained in-house at CyberCX by experts at the company.[70] Academy associates complete training programs that are matched with client work. Although this program has mastered on-the-job-training, if falls short when linking training with formal VET and/or university qualifications.

The Australian Security Intelligence Organisation (ASIO) is the leading government institution responsible for protection against espionage, sabotage, and foreign interference. The information technology department at ASIO offers a 12-month graduate program. Participants work through a rotation of three different disciplines of choice, including information technology and cyber security.[71]

Aside from training and mentoring, participants work on large-scale cyber threat hunting projects with cutting edge technology unique to the ASIO. However, due to the sensitive nature of the projects, most employees require a security clearance – a rather lengthy affair.

The Australian Signals Directorate (ASD) offers a wide range of entry level programs including cadetships and apprenticeships in cyber security.[72] Cadetships give university students an opportunity to work on various projects, including cyber security, whilst receiving mentoring from experienced professionals. Students receive an AU$800 Australian academic allowance per subject completed at university and work part-time for a minimum of two days a week. Upon completion of the program, cadets are offered a full-time position.

ASD apprenticeships consist of four days of work per week, with the rest of apprentices' time dedicated to completing a Certificate IV (two years) or a Diploma (three years). ASD pays for the cost of apprentices' studies, and they receive a competitive remuneration package. In addition to formal studies, apprentices undertake extensive internal training where they obtain additional nationally-recognised qualifications. Both ASD cadetships and apprenticeships offer practical and dynamic work experience for aspiring cyber professionals. Yet, one limitation is their restriction to Australian citizens only, hampering diversity in the successful cohorts of cadets and apprentices.

Finally, the Microsoft Cyber Security Traineeship program is a two-year traineeship run in collaboration with TAFE NSW, Prodigy Learning, MEGT and other industry partners. During their placement, participants attain a Certificate IV in Cyber Security.[73] MEGT acts as a group training organisation and offers ongoing support with training, work health and safety, mentoring and payroll compliance to reduce the costs for participating businesses. MEGT also places prospective candidates with host organisations.

As it stands, graduate programs in cyber security are great initiatives for the development of early-career professionals but require some investment from host organisations. Due to the investment required by industry, it is challenging for small to medium businesses to administer these programs.

International tertiary courses in cyber security

Cyber security is a critical issue internationally, as it is locally. Reports indicate that combined international damages caused by cyber-crime will reach US$10.5 trillion by 2026.[74] In response to the growing demand for skilled cyber security specialists, countries around the world have made substantial investments into innovative training and development initiatives.

International vocational education and training models

Cyber security training in the UK is approached through a degree apprenticeship model – the source of inspiration for this thought leadership report.

The UK program places a student undertaking a certificate, diploma, or bachelor's degree in a cyber-related role in industry for the course of their studies.[75] In doing so, students gain valuable hands-on experience in an area relevant to their studies, while industry partners access a pool of motivated aspiring cyber professionals to meet their business needs.

The implementation of this apprenticeship model varies across different institutions. For instance, at the University of Glasgow in Scotland, cyber apprentices must attend one on campus seminar per week.[76]

All cyber apprenticeships in the UK are credit rated to their Qualifications and Credit Framework.[77] This ensures that there are clear outcomes defined by a recognised framework.

In Israel, the national Defence Force, Ben-Gurion University and industry partners have joined forces to create a Cyber Defence Training School, which teaches both creative problem-solving and advanced technical skills. Comprising 65 per cent practical training and 35 per cent course work, this program is focused on hands-on skills. Individuals from a variety of backgrounds can enter directly into the program via a specialised test.[78]

The UK's apprenticeship model for cyber security training, which combines robust education with industry experience, creates a consistent pipeline of experienced graduates to fill cyber skills gaps in industry. Israel's approach, through a specialised school system with a focus on hands-on skills, is evidence that a practical approach to developing talent in cyber security is feasible. Our proposed cyber degree apprenticeship model is inspired by both these training systems.

Successful international apprenticeship programs

Internationally, there are success stories of apprenticeship-style training models.

German apprenticeships

In Germany, there are more than 300 occupations that are recognised by the German Office of Vocational Education and Training (GOVET) with standards and requirements that determine the split between students' time in the workplace and educational institution.[79] Participants in this program are accredited in their specific area of expertise.

With more than 400,000 companies offering training positions and two-thirds extending apprentice engagements after completion of apprenticeships,[80] the system ensures that there is a consistent pipeline of professionals entering the workforce. Germany also enjoys one of the world's lowest youth unemployment rates.[81]

Swiss apprenticeships

Similarly, in Switzerland apprenticeships are based on a guideline that sets out occupation-specific skills and knowledge mandated at the federal level.[82]

One of the main challenges around apprenticeships are the costs incurred by organisations. Many countries have taken different approaches to addressing this issue. For instance, Switzerland has relaxed regulations around training in a way that allows apprentices to generate enough benefits that ensure that organisations break even when the apprenticeship engagement has ended.[83]

In contrast, Germany has tackled this issue by establishing strict employment regulations, particularly those related to termination of employment, and promoting long-term employment.[84] This has resulted in most apprentices staying with an employer for an extended period after their training concludes.

End notes

1 Australian Financial Review (2023). *How Tom got five-years' training, good pay and a job while studying.* https://www.afr.com/work-and-careers/education/how-tom-got-5-years-training-good-pay-and-a-great-job-while-studying-20231109-p5eivr

2 AustCyber (2023). *SCP - Chapter 3 - The challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development.* https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3

3 Victorian Chamber (2023). *Cyber Security and Scams Policy Position.* https://www.victorianchamber.com.au/policy-and-advocacy/initiatives/cyber-security-and-scams-policy-position

4 UK Cyber Security Council (2023). *Entry routes – regulated qualifications.* https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/entry-routes-regulated-qualifications/

5 Australian Small Business and Family Enterprise Ombudsman (2023). *Small Business Matters.* https://www.asbfeo.gov.au/sites/default/files/2023-12/Small%20Business%20Matters_June%202023_1.pdf

6 Department of Home Affairs (2023). 2023-2030 *Australian Cyber Security Strategy.* https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

7 Australian Signals Directorate (2023). *ASD Cyber Threat Report 2022-2023.* ASD Cyber Threat Report 2022-2023 | Cyber.gov.au

8 Australian Signals Directorate (2022). *ASD Cyber Threat Report 2021-2022.* ASD's ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au

9 Australian Signals Directorate (2021). *ASD Cyber Threat Report 2020-2021.* ACSC Annual Cyber Threat Report - 2020-2021.pdf

10 Australian Signals Directorate (2020). *ASD Cyber Threat Report 2019-2020.* ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

11 Australian Signals Directoriate (2023). *ASD Cyber Threat Report 2022-2023.* https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

12 Australian Signals Directorate (2023). *ASD Cyber Threat Report 2022-2023.* ASD Cyber Threat Report 2022-2023 | Cyber.gov.au

13 ACSC (2020). *Cyber security and small business survey.* https://www.cyber.gov.au/sites/default/files/2023-03/Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results%20-%2020201130.pdf

14 ACSC (2020). *Cyber security and small business survey.* https://www.cyber.gov.au/sites/default/files/2023-03/Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results%20-%2020201130.pdf

15 AustCyber (2023). *Figure -23 Breakdown of job ads by experience requested.* SCP - Chapter 3 - The challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development | AustCyber

16 Australian Government (2023). *Financial support for employers.* https://www.apprenticeships.gov.au/support-and-resources/financial-support-employers

17 Victorian Chamber. (2024). *Federal Budget Submission 2024-25*

18 Microsoft (2023). *Microsoft announces A 5 billion investment in computing capacity and capability to help Australia seize the AI era.* Microsoft announces A$5 billion investment in computing capacity and capability to help Australia seize the AI era – Microsoft Australia News Centre

19 Cyber Wardens (2024). https://cyberwardens.com.au/

20 Australian Signals Directorate (2024). *REDSPICE.* https://www.asd.gov.au/about/what-we-do/redspice

21 Australian Cyber Security Magazine (2022). *Dire Impact of Burnout in Cyber Industry.* https://australiancybersecuritymagazine.com.au/dire-impact-of-burnout-in-cyber-industry/

22 Zednet (2020). *Average tenure of a CISO is just 26 months due to high stress and burnout.* https://www.zdnet.com/article/average-tenure-of-a-ciso-is-just-26-months-due-to-high-stress-and-burnout/

23 UK Cyber security council (2023). *About professional standards.* About Professional Standards (ukcybersecuritycouncil.org.uk)

24 UK Cyber Security Council (2023). *Entry routes – regulated qualifications.* https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/entry-routes-regulated-qualifications/

25 Ministers' treasury portfolio (2023). *Small businesses to receive cyber security boost.* Small businesses to receive cyber security boost | Treasury Ministers

26 Victorian Chamber (2023). *Career Services Policy Paper.* https://www.victorianchamber.com.au/policy-and-advocacy/initiatives/career-services-policy

27 Deloitte (2024). *Cyber Academy.* https://www.deloitte.com/au/en/about/story/impact/cyber-academy-developing-australia-cyber-talent-future.html

28 Crowdstrike (2023). *Red team vs Blue team.* Red Team VS Blue Team: What's the Difference? - CrowdStrike

29 Crowdstrike (2023). *Red team vs Blue team.* Red Team VS Blue Team: What's the Difference? - CrowdStrike

30 Paul Jerimy (2023). *Security Certification Roadmap.* https://pauljerimy.com/security-certification-roadmap/

31 Amazon Web Services (2023). *AWS certified cloud Practitioner.* https://aws.amazon.com/certification/certified-cloud-practitioner/

32 Amazon Web Services (2023). *Learn from our customers.* https://aws.amazon.com/government-education/worldwide/australia-new-zealand/

33 Microsoft (2023). *Microsoft Certified: Azure Fundamentals.* https://learn.microsoft.com/en-us/certifications/azure-fundamentals/

34 Microsoft (2023). *Microsoft Certified: Azure Security Engineer Associate.* https://learn.microsoft.com/en-us/certifications/azure-security-engineer/?wt.mc_id=learningredirect_certs-web-wwl

35 TCM (2023). *Practical network Penetration Tester.* Practical Network Penetration Tester - TCM Security (tcm-sec.com)

36 CompTIA (2023). *CompTIA PenTest+.* https://www.comptia.org/certifications/pentest

37 SANs (2023). *SEC560: enterprise penetration testing.* SEC560: Enterprise Penetration Testing Course | SANS Institute

38 GIAC (2023). *GIAC strategic policy, planning, and leadership certification.* GIAC Strategic Planning, Policy, and Leadership | Cybersecurity Certification

39 Australian government (2023). *HECS-HELP.* HECS-HELP - StudyAssist, Australian Government

40 AustCyber (2023). *Lack of skilled workers is not the only cause of the skills shortage.* SCP - Chapter 3 - The challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development | AustCyber

41 Thomas Deissinger and Phillip Gonon (2020). *The development and cultural foundations of dual apprenticeships - a comparison of Germany and Switzerland.* Full article: The development and cultural foundations of dual apprenticeships – a comparison of Germany and Switzerland (tandfonline.com)

42 Samuel Muehlemann and Stefan C Wolter (2014). *Return on investment of apprenticeship systems for enterprises: Evidence from cost-benefit analyses.* 2193-9004-3-25.pdf (springer.com)

43 TAFE NSW (2023). *TAFE NSW Cyber Academy Student kicks goals on world stage.* https://www.tafensw.edu.au/media/-/blogs/tafe-nsw-cyber-academy-student-kicks-goals-on-world-stage

End notes

44 Apprenticeships Support Australia (2023). *About us*. https://www.apprenticeshipsupport.com.au/About-Us

45 Victorian Chamber of Commerce and Industry (2023). *Cyber Security and Scams Policy Position*. https://www.victorianchamber.com.au/policy-and-advocacy/initiatives/cyber-security-and-scams-policy-position

46 Busy sisters (2023). *Our program*. https://busysisters.com.au/about-us/

47 Genius Armoury (2024). https://geniusarmoury.com/

48 L.E Potter, G Vickers (2023). *What Skills do you Need to Work in Cyber Security? A Look at the Australian Market*. https://dl.acm.org/doi/abs/10.1145/2751957.2751967

49 Monash University (2023). *Information Technology*. https://www.monash.edu/study/courses/find-a-course/information-technology-c2000

50 Deakin university (2023). *Information technology placements: sit344*. https://www.deakin.edu.au/students/study-support/faculties/sebe/student-support/work-integrated-learning/information-technology

51 Deakin university (2023). *Team capstone project*. https://www.deakin.edu.au/courses/unit?unit=SIT374

52 Deakin university (2023). *Information technology placements: sit306*. https://www.deakin.edu.au/students/study-support/faculties/sebe/student-support/work-integrated-learning/information-technology

53 The University of Melbourne. *Computer science*. https://study.unimelb.edu.au/find/study-areas/computer-science/

54 The University of Melbourne (2023). *Computing and software systems*. https://study.unimelb.edu.au/find/courses/undergraduate/bachelor-of-science/

55 The University Of Melbourne (2023). *Students@work Internship Program*. https://students.unimelb.edu.au/careers/find-a-job/working-on-campus/students@work-internship-program

56 RMIT University (2023). *Bachelor of Information technology*. https://www.rmit.edu.au/study-with-us/levels-of-study/undergraduate-study/bachelor-degrees/bp162?ef_id=EAIaIQobChMI7rPht7DbgAMVJhKDAx0bkwi2EAAYASAAEgIRMvD_BwE:G:s&s_kwcid=AL!14937!3!652762824457!b!!g!!bachelor%20of%20information%20technology!19898452221!148097424912&cq_plac=&cq_net=g&cq_pos=&cq_med=&cq_plt=gp&gad=1&gclid=EAIaIQobChMI7rPht7DbgAMVJhKDAx0bkwi2EAAYASAAEgIRMvD_BwE&gclsrc=aw.ds

57 TAFE Victoria (2023). *Free tafe for more Victorians*. Free TAFE for more Victorians | vic.gov.au (www.vic.gov.au)

58 RMIT University (2023). *Certificate IV in cyber security*. https://www.rmit.edu.au/study-with-us/levels-of-study/vocational-study/certificates/certificate-iv-in-cyber-security-c4424

59 Federation University (2023). *Bachelor of IT (professional practice)*. Bachelor of Information Technology (Professional Practice) - Federation University Australia | Study

60 Ai group (2023). *Innovative partnership between IBM & Federation University yields significant economic benefits*. https://www.aigroup.com.au/education-training/centre-for-education-and-training/blog/innovative-partnership-between-ibm--federation-university-yields-significant-economic-benefits/

61 Ai group (2023). *Innovative partnership between IBM & Federation University yields significant economic benefits*. https://www.aigroup.com.au/education-training/centre-for-education-and-training/blog/innovative-partnership-between-ibm--federation-university-yields-significant-economic-benefits/

62 Swinburne (2023). *Diploma of Information Technology (Advanced Networking Cyber Security) VIC Cyber Academy*. https://www.swinburne.edu.au/course/tafe/diploma-of-information-technology-advanced-networking-cyber-security-cyber-academy-ict50220/

63 TAFEcyber (2023). *About TAFEcyber*. https://www.tafecyber.com.au/about

64 TAFE Victoria (2023). *FreeTAFE for more Victorians*. Free TAFE for more Victorians | vic.gov.au (www.vic.gov.au)

65 Victorian Government (2023). *Digital Jobs*. https://djsir.vic.gov.au/digital-jobs/businesses

66 Box Hill institute (2023). *Certificate IV in Cyber-security*. https://www.boxhill.edu.au/courses/certificate-iv-in-cyber-security-ct423-d/

67 Victoria university (2023). *THABC Cybersecurity Essentials*. https://www.vu.edu.au/courses/cybersecurity-essentials-thabc#OPEN-MODAL

68 TAFEcyber (2023). *Essential Eight Assessment Course*. https://www.tafecyber.com.au/essential-eight

69 EY (2023). *Cybersecurity student opportunities*. https://www.ey.com/en_au/careers/cybersecurity-student-opportunities

70 CyberCX (2023). *CyberCX Academy*. https://cybercx.com.au/cybercxacademy/

71 ASIO (2023). *Graduates*. https://www.asio.gov.au/careers/graduates

72 Australian Signals Directorate (2024). *I'm starting my career*. https://www.asd.gov.au/careers/im-starting-my-career#:~:text=A%20cadetship%20is%20for%20university,upon%20successfully%20completing%20your%20subjects.

73 MEGT (2023). *Cyber Security Microsoft traineeship program*. https://www.megt.com.au/microsoft-traineeship-program/cyber-security-program/employers

74 Forbes (2023). *10.5 Trillion Reasons Why We Need A United Response To Cyber Risk*. 10.5 Trillion Reasons Why We Need A United Response To Cyber Risk (forbes.com)

75 Cyber Security Council United Kingdom (2023). *Entry routes – related qualifications*. https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/entry-routes-regulated-qualifications/

76 Glasgow Caledomain univeisty (2023). *Graduate Apprenticeship Cyber Security*. Graduate Apprenticeship Cyber Security | Glasgow Caledonian University | Scotland, UK (gcu.ac.uk)

77 Jim Horden (2015). *Degree apprenticeships in England: professional and vocational formation*. Degree apprenticeships in England: professional and vocational formation: International Journal of Training Research: Vol 13, No 3 (tandfonline.com)

78 DefenseNews (2023). *How Israel is preparing the next generation of cyber soldiers*. https://www.defensenews.com/interviews/2022/11/29/how-israel-is-preparing-the-next-generation-of-cyber-soldiers/

79 Expatrio (2023). *The German Dual apprenticeship system*. German dual apprenticeship system | Expatrio.com.

80 Expatrio (2023). *The German Dual apprenticeship system*. German dual apprenticeship system | Expatrio.com.

81 OECD data (2023). *Youth Unemployment rate*. Unemployment - Youth unemployment rate - OECD Data

82 Thomas Deissinger and Phillip Gonon (2020). *The development and cultural foundations of dual apprenticeships - a comparison of Germany and Switzerland*. Full article: The development and cultural foundations of dual apprenticeships – a comparison of Germany and Switzerland (tandfonline.com)

83 Wolter, Stefan and Joho, Eva (2018). *Apprenticeship training in England: a cost-effective model for firms?*. Apprenticeship training in England: a cost-effective model for firms? - Archive of European Integration (pitt.edu)

84 Wolter, Stefan and Joho, Eva (2018). *Apprenticeship training in England: a cost-effective model for firms?*. Apprenticeship training in England: a cost-effective model for firms? - Archive of European Integration (pitt.edu)

Victorian Chamber of Commerce and Industry

The Victorian Chamber of Commerce and Industry (VCCI) is the largest and most influential not-for-profit business organisation in Victoria, informing and servicing more than 85,000 members and clients across the State.

Through our policy and advocacy work, professional development courses, workplace relations and consulting services, we help thousands of businesses every year to improve workplace performance and achieve business growth and success.

Victorian Chamber of Commerce and Industry | 150 Collins Street, Melbourne VIC 3000 | Phone 03 8662 5333

Victorian Chamber of Commerce and Industry

#vcci

The Victorian Chamber of Commerce and Industry,
150 Collins Street, Melbourne, Victoria 3000
Phone: (03) 8662 5333 victorianchamber.com.au March 2024

victorianchamber.com.au