Bridging the Cybersecurity Skills Gap: A Call to Action for Australia's Vocational Education and Training Sector.

Paul Goudie

Victorian Skills Authority Fellowship, 2024

International Specialised Skills Institute

Victorian Skills Authority

First Published 2024

Disclaimer: The Victorian Skills Authority (VSA) provides financial support to the International Specialised Skills (ISS) Institute under a grant agreement to support ISS Institute Fellows' research activities. Although the VSA has provided financial support for this research, the research produced is not a statement of Victorian Government policy. The Victorian Government provides no endorsement of the research's content, findings or conclusions. By sharing this research, VSA makes no representation about the Victorian Government's intention to implement any conclusions or findings identified in the research.

Report by Paul Goudie
Typeset by Danielle Cull
Printed by MDM Copy Centre

The International Specialised Skills Institute

1/189 Faraday St,
Carlton VIC 3053
info@issinstitute.org.au
+61 03 9347 4583

ISBN: 978-1-923027-67-1

Table of contents

01 Acknowledgements

The Awarding Bodies

The Fellow sincerely thanks the Victorian Skills Authority (VSA) for providing funding support for the ISS Institute and for this Fellowship.

The ISS Institute plays a pivotal role in creating value and opportunity, encouraging new thinking and early adoption of ideas and practice by investing in individuals. The overarching aim of the ISS Institute is to support the development of a 'Better Skilled Australia'. The Institute does this via the provision of Fellowships that allow Australians to undertake international skills development and applied research that will positively impact Australian industry and the broader community.

The ISS Institute was founded in 1991 by a small group of innovators, including Sir James Gobbo AC, CVO, QC, and former Governor of Victoria, who had a vision of building a community of industry specialists who would lead the up skilling of the Australian workforce.

The Fellowship program builds shared learning, leadership, and innovation across the broad range of industry sectors worked with. Fellows are supported to disseminate learning and ideas, facilitate change and advocate for best practices by sharing their Fellowship learnings with peers, colleagues, government, industry, and community. Since its establishment, ISS Institute has supported over 580 Fellows to undertake skill and knowledge enhancement across a wide range of sectors which has led to positive change, the adoption of best practice approaches and new ways of working in Australia.

The Fellowship programs are led by our partners and designed to achieve the needs and goals desired by the partners. ISS Institute works closely to develop a Fellowship program that meets key industry priorities, thus ensuring that the investment will have a lasting impact.

For further information on ISS Institute Fellows, refer to www.issinstitute.org.au

Governance and Management

- **Patron in Chief:** Lady Primrose Potter AC
- **Patrons:** Mr Tony Schiavello AO, Mr James MacKenzie and Mark Kerr
- **Founder:** Sir James Gobbo AC, CVO
- **Board Chair:** Professor Amalia Di Iorio AM
- **Board Treasurer:** Adrian Capogreco
- **Board Secretary:** Alisia Romanin
- **Board Members:** Jeremy Gobbo KC and Vicki Abraham
- **Chief Executive Officer:** Dr Katrina Jojkity

Sponsor - the Victorian Skills Authority

The Victorian Skills Authority works in partnership with the International Specialised Skills Institute by funding the VET International Practitioner Fellowships. The Fellowship program focuses on developing opportunities within the VET sector to assist in building an Education State in Victoria that produces excellence and reduces the impact of disadvantage. In addition, the program is funded to support the priorities of Skills First, including developing capacity and capability, innovative training practices and increasing teacher quality within the VET sector as well as building industry capability and developing Victoria's current and future workforce.

Fellow's acknowledgements

The Fellow extends sincere thanks to Katrina Jojkity, Chief Executive of the ISS Institute, Kay Schlesinger, Program Manager, and others for their invaluable support. Acknowledgment is also due to the Victorian Skills Authority (VSA) and Swinburne University of Technology for their essential roles in supporting the Fellow's International VET Practitioner Fellowship.

02

The Fellow's Reflection on Pursuing the Fellowship

Motivated by a deep interest in cybersecurity, the Fellow pursued this Fellowship to explore how the VET sector can address industry skills shortages. Building strong connections between vocational educational institutions and industry stakeholders is essential for addressing the cybersecurity skills gap. Integrating emerging technologies and current industry trends into the curriculum is crucial to keeping training package competencies relevant. This will ensure students acquire the most up-to-date, job-ready skills and knowledge to tackle real-world cybersecurity challenges.

The Fellowship represents a key milestone in the Fellow's professional development. It provided an opportunity to enhance knowledge in the rapidly changing field of cybersecurity, which constantly evolves with threats and innovative countermeasures. Serving as an ISS Fellow has significantly influenced the Fellow's professional growth by expanding their network. The Fellowship enabled the Fellow to connect and engage with leading cybersecurity professionals worldwide. This has resulted in valuable connections and opened doors to opportunities and professional relationships beyond the duration of the Fellowship.

The Fellowship aligns with the Fellow's passion for workforce development, bridging industry skills gaps through education. Vocational education equips students with practical, job-ready skills, contributing to a skilled workforce capable of addressing real-world challenges (Hong, C., 2022). As an advocate for applied learning, the Fellow values the VET sector's role in preparing industry-ready professionals. The Fellowship facilitated knowledge exchange and enriched students' experiences at the Fellow's prior employer, Swinburne University. This ensures they are well-prepared to tackle cybersecurity threats and contribute significantly to Australia's cybersecurity landscape.

The Fellowship has significantly enhanced the Fellows' visibility within the education sector, industry, and the media to highlight the cybersecurity skills gap. The Fellow was profiled in web articles, email newsletters, and even a Seven Nightly News segment on cybersecurity. These platforms enabled valuable connections with cybersecurity experts across academia, industry and Government, which have been pivotal in shaping the Fellow's learning journey. With this learning, the Fellow is enthusiastic about applying the skills they have acquired to improve cybersecurity more broadly in the VET sector. Additionally, the Fellowship has broadened the Fellow's understanding of strategies to address the broader skills gap in industries affected by such shortages, such as aged care and early learning.

Pursuing this Fellowship has been an enriching professional and personal development journey. It aligns with the Fellow's passion for cybersecurity and workforce development, enabling them to implement what they have learned to bridge the cybersecurity skills gap.

03 Introduction

Australia aims to become the leading cyber-secure nation in the evolving global cybersecurity landscape by 2030 (Australian Government, 2023). This aspiration underscores the critical importance of cybersecurity in safeguarding the nation's digital infrastructure against an increasing array of cyber threats. At the heart of this strategic vision lies a significant challenge—the cybersecurity skills gap.

This Fellowship report examines the VET sector's challenges in developing a cybersecurity workforce and outlines potential strategies for bridging this gap. The report identifies vital barriers within the current educational framework, such as outdated curricula, limited practical training opportunities, and variable engagement between vocational educational institutions and the cybersecurity industry.

Moreover, this report explores the value of enhanced educational-industry partnerships in improving the quality and accessibility of cybersecurity education. Such collaborations are crucial in aligning educational outcomes with industry needs, ensuring that graduates possess the relevant skills and knowledge to address contemporary cybersecurity challenges.

This report examines the impacts of these initiatives in detail and highlights the transformative potential of effectively addressing the cybersecurity skills gap. By improving the alignment between vocational education and industry requirements, these efforts can bolster employment opportunities for Victoria graduates and enhance Australia's cybersecurity infrastructure's overall resilience and capability.

Furthermore, the report emphasises the need for continuous professional development and lifelong learning opportunities for VET practitioners and educators to keep pace with the rapidly evolving cybersecurity landscape. It advocates for implementing innovative teaching methodologies and cutting-edge technologies within the educational framework to create a dynamic and responsive learning environment.

In summary, this Fellowship Report presents a comprehensive analysis of the current state of cybersecurity education within the vocational sector and offers actionable considerations for closing the skills gap. The report identifies critical opportunities to develop a skilled cybersecurity workforce through Australia's VET system by fostering a collaborative approach between Government, industry, and educational institutions. It examines challenges to the state's cybersecurity framework and the broader Australian cyber ecosystem, proposing strategic interventions to enhance the quality and accessibility of cybersecurity education within Victoria. Implementing these measures will establish a robust and adaptable cybersecurity workforce to safeguard Australia's digital future.

04

Unlocking Potential: How the Vocational Education System Can Bridge the Cybersecurity Skills Gap

Australia's VET framework is vital in addressing the shortage of cybersecurity skills by equipping learners with essential technical skills and knowledge. A recent review by Deloitte of ICT and cybersecurity qualifications across major TAFE (Technical and Further Education) providers revealed comprehensive programs covering essential cybersecurity knowledge and general ICT skills. Since 2017, the introduction of focused postgraduate qualifications has offered pathways for professionals transitioning into cybersecurity. TAFECyber aims to enhance the relevance and accessibility of TAFE cybersecurity programs.

However, according to data from the National Centre for Vocational Education Research (NCVER), many students who complete their studies are international students who may return to their home countries (NCVER, 2023). Despite this, the data shows high satisfaction among graduates (71.2%) and a median salary of $57,400, with 39% of graduates working in professional or technical services after completing their studies. Increased promotion and advocacy could showcase the benefits of these qualifications.

A vocational pathway is essential for building a skilled cybersecurity workforce capable of meeting the evolving demands of the digital era. Yet, various challenges constrain the system's effectiveness. Structural issues such as a lack of coordination among VET providers and duplication of efforts hinder resource allocation and standardisation. This makes it difficult for students to choose the right program and for employers to assess potential employees' skills (European Training Foundation, 2024). In addition, technological advancements require constant updating of curriculum and training methods, which can be costly and time-consuming for VET providers.

VET providers must collaborate with industry experts and employers to overcome these challenges and develop relevant and up-to-date curricula. This will ensure that students have the necessary skills and knowledge to meet industry demands. Additionally, partnerships between VET providers and businesses can offer valuable opportunities for students to gain practical experience through internships or apprenticeships.

Government support is crucial in strengthening the VET system. In addition to collaborating with industry, adequate funding must be provided to improve infrastructure, acquire modern technology and equipment, and recruit well-qualified VET practitioners. This will attract more students to enrol in VET courses and ensure their training is high quality and relevant to current industry standards.

Another critical aspect of a successful VET system is providing student support services. These can include career counselling, mentoring programs, and financial assistance for those who may face barriers to accessing education.

By addressing these challenges early on, we can help ensure that the VET sector continues to play a critical role in closing the cybersecurity skills gap now and in the future.

05

The state of cybersecurity in Victoria: An overview

The cybersecurity landscape in Victoria is influenced by the Victorian Government's 2021 Digital Strategy, which prioritises reducing cyber risks and enhancing digital service delivery throughout the state (Victorian Government, 2021). This strategy uses advanced technology to provide efficient and tailored services while safeguarding against emerging cyber threats. However, the challenge for the cybersecurity sector is that policies released in 2021 have quickly become outdated in the rapidly evolving cybersecurity environment. New threats and changing technology require strategies and measures to adapt to remain effective.

The 2021 Digital Strategy recommended adopting agile regulatory frameworks to keep up with the rapidly changing cyber threat landscape. The Victorian Government seeks to improve its cybersecurity resilience and capabilities by establishing clear guidelines and protocols to set a standard for other regions. The strategy also highlights the importance of public-private partnerships in enhancing cybersecurity. These partnerships promote knowledge sharing and resource pooling, leading to a more comprehensive and coordinated response to cyber threats. This collaborative approach is crucial for creating a secure digital environment capable of withstanding sophisticated cyber-attacks.

This is where collaboration between Government, industry, and the VET sector plays a crucial role. By working together, these sectors can share knowledge and resources to constantly update and improve cybersecurity practices in Victoria. The Government can provide funding for research and development, while industry experts can offer expertise on emerging threats and solutions. Meanwhile, the VET sector can train the next generation of cybersecurity professionals and equip them with the skills needed to keep up with the ever-changing landscape.

The Victorian Government prioritises strengthening its cyber resilience by partnering with key stakeholders. These partnerships promote information sharing, develop innovative solutions, and enhance cyber defence capabilities. Another significant focus of the strategy is to promote digital inclusion, ensuring equitable access to digital tools and services for all citizens. This inclusivity is crucial as it supports a broad base of educated users who are aware of cybersecurity best practices, thereby reducing vulnerabilities stemming from human error. The Government aims to build a strong foundation for a secure cyber ecosystem by fostering an inclusive digital environment.

Investing in skills development is critical to Victoria's evolving cybersecurity strategy. The Free TAFE program now includes Certificate IV in Cybersecurity, a significant step towards closing the skills gap. This initiative promotes partnerships between Government, private sector, and educational institutions to build a workforce ready to address cyber threats. By aligning education with industry needs, Victoria aims to cultivate a skilled workforce capable of meeting cybersecurity challenges head-on.

In summary, Victoria’s cybersecurity state is characterised by an inclusive, collaborative, and strategically focused approach, as outlined in the 2021 Digital Strategy. By investing in skills development, implementing agile regulatory frameworks, and fostering public-private partnerships, Victoria is making significant strides toward securing its digital future. This proactive stance enhances the security of digital operations within businesses and Government agencies and contributes to the overall safety and resilience of the state’s digital infrastructure.

06

The Fellow's Research Methodology

During the Fellowship, the Fellow utilised a research methodology focused on immersing in the cybersecurity ecosystem in Australia and internationally. This involved attending leading industry conferences and conducting interviews with recognised cybersecurity experts. This approach ensured a comprehensive understanding of global cybersecurity and provided valuable insights into the challenges faced by Australia's VET sector.

Additionally, the Fellow engaged with various stakeholders, including Government agencies, educational institutions, and industry associations, to gain a well-rounded perspective on the current landscape and potential solutions for addressing the growing need for a robust and adaptable cybersecurity workforce.

The Fellow continuously reviewed emerging technology trends to ensure the accuracy and relevance of findings in cybersecurity education, providing informed considerations for preparing future students.

The information gathered from these professional interactions was crucial in directing the research and setting the stage for developing strategic considerations. The upcoming sections will detail the activities undertaken during the Fellowship and emphasise how they contributed to achieving the research objectives. A subsequent analysis will highlight the key findings from these initiatives and their impact on enhancing cybersecurity education within the VET system in Australia.

07

The Role and Impact of Attending Conferences in Applied Cybersecurity Research

As part of the Fellow's applied research for this Fellowship, attending several key conferences has been instrumental in deepening their understanding of the cybersecurity skills gap. These conferences, including the Global Cyber Conference in Zurich, the Cybersecurity Skills Conference organised by the European Union Agency for Cybersecurity (ENISA), and EDTECH WEEK in New York City, provided unique platforms for engaging with leading cybersecurity experts and practitioners. The Fellow also attended the National Tech Summit, the annual flagship event of the Tech Council of Australia (TCA) that brought together established and emerging leaders across Australia's tech ecosystem.

Attending these conferences also facilitated invaluable networking opportunities. Engaging with peers and experts allowed for exchanging ideas and best practices, fostering collaborative relationships that extend beyond the duration of the events. These connections are crucial for ongoing research and development efforts, providing access to broader knowledge and resources.

Conferences serve as a valuable medium for knowledge exchange, offering opportunities to hear firsthand from global thought leaders about the latest cybersecurity trends, challenges, and innovations. Participating in these events gave the Fellow valuable insights into the current state of cybersecurity practices and the evolving threat landscape. This exposure is essential for applied research as it ensures that findings and considerations are grounded in the most recent developments within the industry.

At the Global Cyber Conference in Zurich, discussions focused on emerging cyber threats and advanced strategies to counter them, highlighting the need for specialised skills and continuous professional development in cybersecurity. The Cybersecurity Skills Conference by ENISA provided a detailed analysis of the skills gap within the European context, emphasising collaborative efforts between Governments, industry, and educational institutions to address training deficiencies and cultivate a competent workforce. EDTECH WEEK in New York City intersected education technology with cybersecurity, showcasing innovative teaching methodologies and technological tools to enhance cybersecurity education. Interactions with specialists underscored the potential of leveraging edtech solutions to provide effective and scalable training programs pertinent to addressing the acute shortage of skilled cybersecurity professionals.

In conclusion, attending these high-profile conferences has significantly enriched the applied research conducted by the Fellow. The insights and experiences gained have been pivotal in understanding the depth and breadth of the cybersecurity skills gap. By integrating the knowledge acquired from these events, this report aims to present well-informed strategies to enhance cybersecurity education and workforce development, ultimately contributing to a more secure digital landscape.

1. The Fellow's Experience at the Global Cyber Conference, Zurich, Switzerland

Attending the Global Cyber Conference in Zurich, Switzerland, in September 2023 was a significant first step in the Fellow's mission to address Australia's cybersecurity skills gap. Recognised as a leading international event, the conference brought together outstanding cybersecurity professionals from across the globe, offering a unique platform to explore advanced security topics such as cloud security and the integration of artificial intelligence in cybersecurity frameworks.

The event featured engaging panel discussions and insightful presentations, highlighting the changing landscape of cyber threats and the crucial need for robust cybersecurity defences. These discussions revealed the various challenges nations and organisations face in protecting themselves against these threats, underscoring the essential role of skilled cybersecurity experts in developing effective protection strategies.

For the Fellow, attending the conference was extremely valuable. It provided a comprehensive understanding of the global outlook on cybersecurity, identified effective educational strategies, and emphasised the significance of collaboration between academia, the corporate sector, and Government entities in building a proficient cybersecurity workforce. The information shared during the event highlighted the urgent need for innovative training approaches and the benefits of a coordinated effort to improve cybersecurity education and workforce preparedness in Australia.

One key takeaway was the critical role of skilled cybersecurity experts in improving the recruitment process of new cybersecurity graduates. This includes technical knowledge and soft skills such as communication, problem-solving, and critical thinking. Another important point raised was the importance of diversity in the cybersecurity field. It was shared that diversity, including gender, cultural, and educational background, brings different perspectives and ideas to problem-solving. This is especially important in cybersecurity, requiring a strong team-based approach. Speakers also discussed various initiatives being implemented by Government entities to support cybersecurity education and workforce development. These initiatives include scholarships for students pursuing degrees in cybersecurity and internships with top companies.

The conference emphasised the importance of investing in education and training programs for current and future cybersecurity professionals and promoting collaboration between sectors to combat cyber threats effectively. The insights gained have been crucial in shaping the Fellow's considerations for strengthening Australia's cybersecurity education framework. A solid foundation can be built to address Australia's increasing cybersecurity needs by combining innovative educational strategies with a united, collaborative effort. This approach is essential to achieving Australia's goal of becoming the most cyber-secure nation in the world by 2030, ensuring a resilient and secure digital future.

GLOBAL CYBER CONFERENCE
ZURICH EDITION
THE DOLDER GRAND | 14–15 SEPTEMBER 2023
Prioritising Cyber Resilience
SWISS CYBER INSTITUTE

Figure 1. Meeting Samir Aliyev, the Founder and CEO of the Swiss Cyber Institute in Zurich, at the Global Cyber Conference.

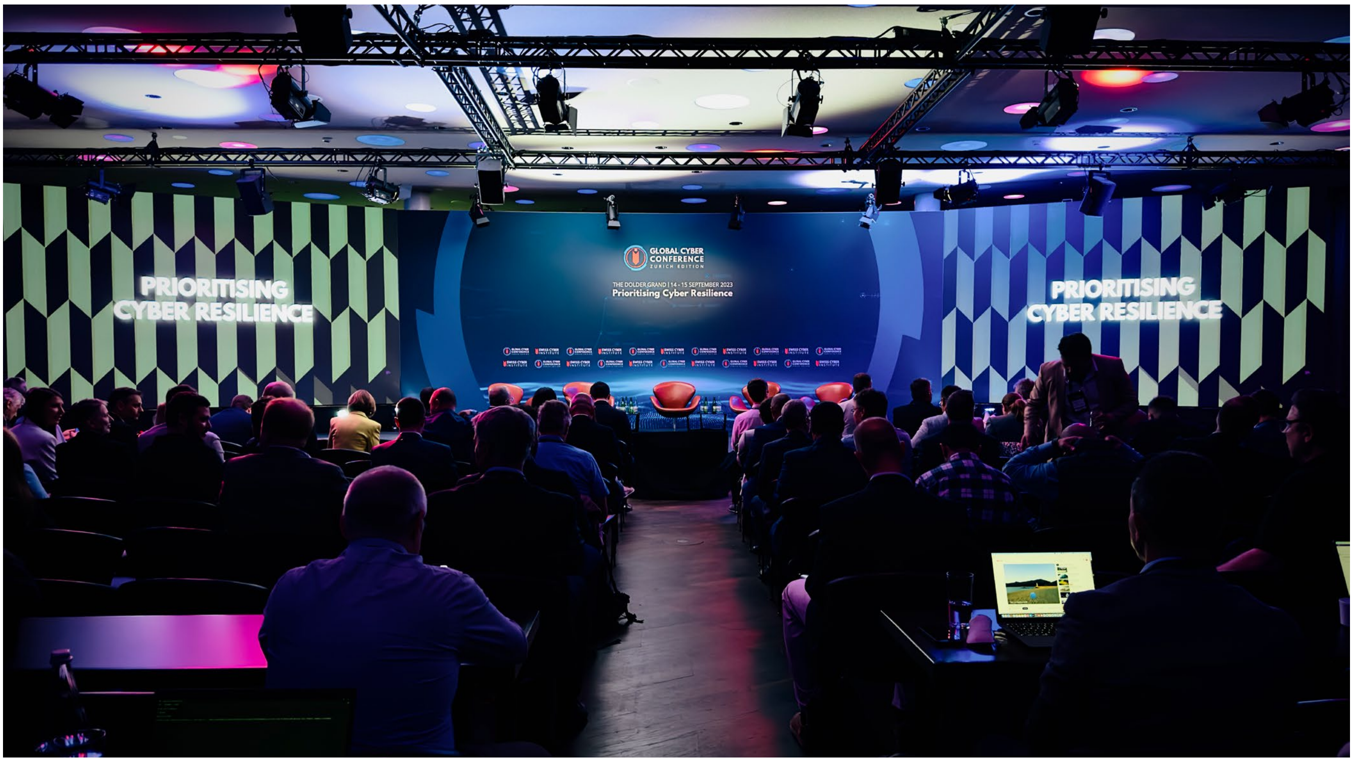

PRIORITISING CYBER RESILIENCE
GLOBAL CYBER CONFERENCE ZURICH EDITION
THE DOLDER GRAND | 14 - 15 SEPTEMBER 2023
Prioritising Cyber Resilience
PRIORITISING CYBER RESILIENCE

Figure 2. Opening session at the Global Cyber Conference, Zurich, Switzerland

Is your cyber strategy too complex to deal with agile attackers?
Together, we see Cybersecurity with different eyes.
The better the question. The better the answer. The better the world works.
EY
Building a better working world

Figure 3. The Global Cyber Conference in Zurich, Switzerland, provided the opportunity for the Fellow to engage with and discuss with many leading commercial operators in the cybersecurity field. EY's Cybersecurity, strategy, risk, compliance, and resilience practice was present, and the Fellow engaged in discussions about organisational cyber risk and capabilities.

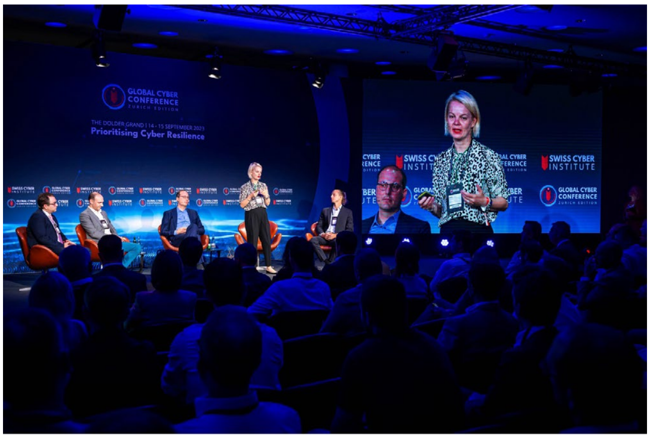

GLOBAL CYBER CONFERENCE ZURICH EDITION
THE DOLDER GRAND | 14 - 15 SEPTEMBER 2023
Prioritising Cyber Resilience
SWISS CYBER INSTITUTE

Figure 4. The Fellow was incredibly fortunate to learn from many global leaders in cybersecurity. Speaking on Cyber Resilience was Dr. Anna Zeiter, the Chief Privacy Officer and Associate General Counsel for Privacy, Data, and AI of eBay Inc. Dr. Zeiter holds a PhD in free speech and fundamental rights from the University of Hamburg and an LL.M. in Law, Science, and technology from Stanford Law School.

2. 2nd European Cybersecurity Skills Conference, Segovia, Spain

In September 2023, the Fellow participated in the Cybersecurity Skills Conference organised by the European Union Agency for Cybersecurity (ENISA). This conference focused on enhancing the skills of individuals in the field of cybersecurity across the EU.

The conference brought together a panel of leading experts, decision-makers, educators, and business representatives to discuss best practices for improving cybersecurity skills and teaching methods. One of the highlights was learning about the National Initiative for Cybersecurity Education Framework (NICE). The NICE Cybersecurity Workforce Framework is the foundation for enhancing the size and capability of the U.S. security workforce. It provides a standard definition of cybersecurity, a comprehensive list of tasks, and the necessary knowledge, skills, and abilities to perform those tasks. Educators and policymakers can use the Framework to set standards to promote workforce professionalisation.

The National Institute of Standards and Technology (NIST) developed the NICE Framework. Many European countries have adopted this framework as a guideline for building a skilled cybersecurity workforce (NIST, 2020). The conference discussed how educational providers can create job-aligned learning programs, ensuring that students graduate with skills needed by employers. Additionally, the conference focused on how employers can recruit more qualified candidates and how employees can have portable skills and well-defined career paths.

Like the Global Cyber Conference in Zurich, the conference highlighted the lack of diversity in cybersecurity, with women making up only 20% of the workforce and minority groups also being underrepresented. To address this issue, several initiatives were discussed, including mentorship programs and outreach efforts to encourage more diversity in the field. Speakers emphasised the importance of promoting diversity within the cybersecurity industry, noting that a diverse workforce brings varied perspectives and innovative solutions to combat cyber threats, especially as the demand for skilled professionals grows.

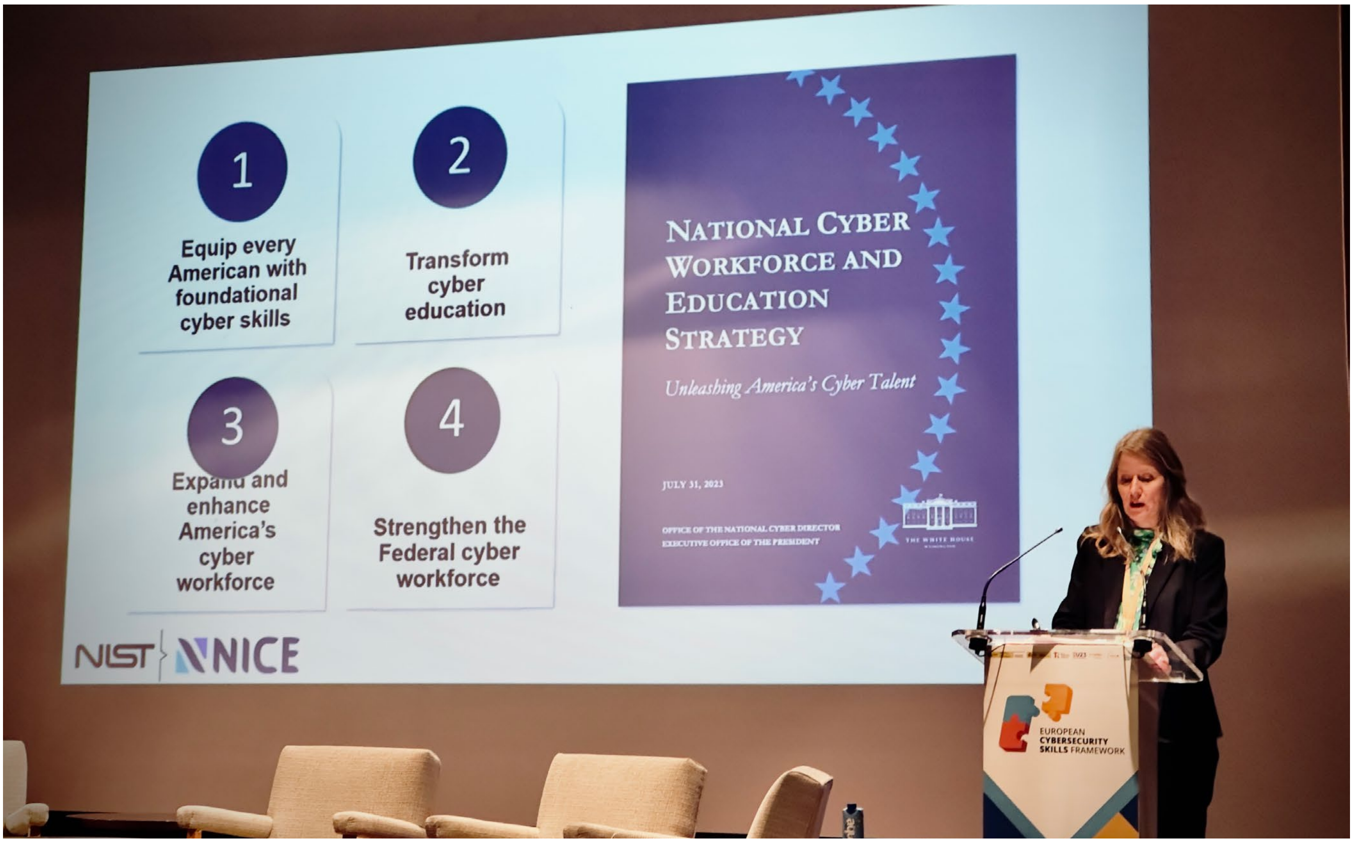
Another topic covered was the increasing significance of soft skills in cybersecurity roles. Along with technical expertise, professionals in this field must have strong communication, leadership, and problem-solving skills. Cybersecurity now involves implementing technology solutions and understanding and managing human behaviour and processes. The conference also discussed emerging trends in the cybersecurity industry, including the use of Artificial Intelligence (AI) and Machine Learning (ML) for threat detection and response. As cyber threats evolve, vocational and university courses play a crucial role in teaching foundational skills that students can build on to acquire advanced technological knowledge for preventing potential attacks.

The insights from the ENISA Cybersecurity Skills Conference are highly relevant to Australia's vocational education sector. For example, the NICE Framework is a valuable model for Victorian educational institutions to align learning outcomes with a competency framework. By adopting similar guidelines, these institutions can ensure that their curricula align with industry needs and standards, producing well-prepared graduates for the workforce. Furthermore, the emphasis on diversity at the conference highlights the need for inclusive educational strategies within Victoria's vocational sector. Implementing mentorship programs and outreach efforts can attract a broader range of students to cybersecurity courses, enriching the talent pool with diverse perspectives. This approach supports social equity and enhances innovation and effectiveness in tackling cyber threats.

The emphasis on soft skills highlights the challenge of vocational training focused on competencies. Communication, leadership, problem-solving modules, and technical training can better equip students for cybersecurity challenges. By developing these competencies, vocational education providers can produce well-rounded professionals capable of navigating the multifaceted nature of cybersecurity work. Moreover, the discussions on AI and ML highlight the need for vocational programs to stay current with technological advancements. Integrating these cutting-edge topics into the curriculum will prepare students to leverage AI and ML tools effectively, positioning them at the forefront of the job market.

By aligning with global best practices and embracing a comprehensive, inclusive approach to education, Australia's vocational sector can significantly contribute to bridging the cybersecurity skills gap. This alignment is vital for meeting the region's cybersecurity needs and supporting Australia's broader goal of becoming the most cyber-secure nation in the world by 2030.

Figure 5. The Fellow at Day One of the 2nd European Cybersecurity Skills Conference, Segovia, Spain



1 Equip every American with foundational cyber skills

2 Transform cyber education

3 Expand and enhance America's cyber workforce

4 Strengthen the Federal cyber workforce

NIST | NICE

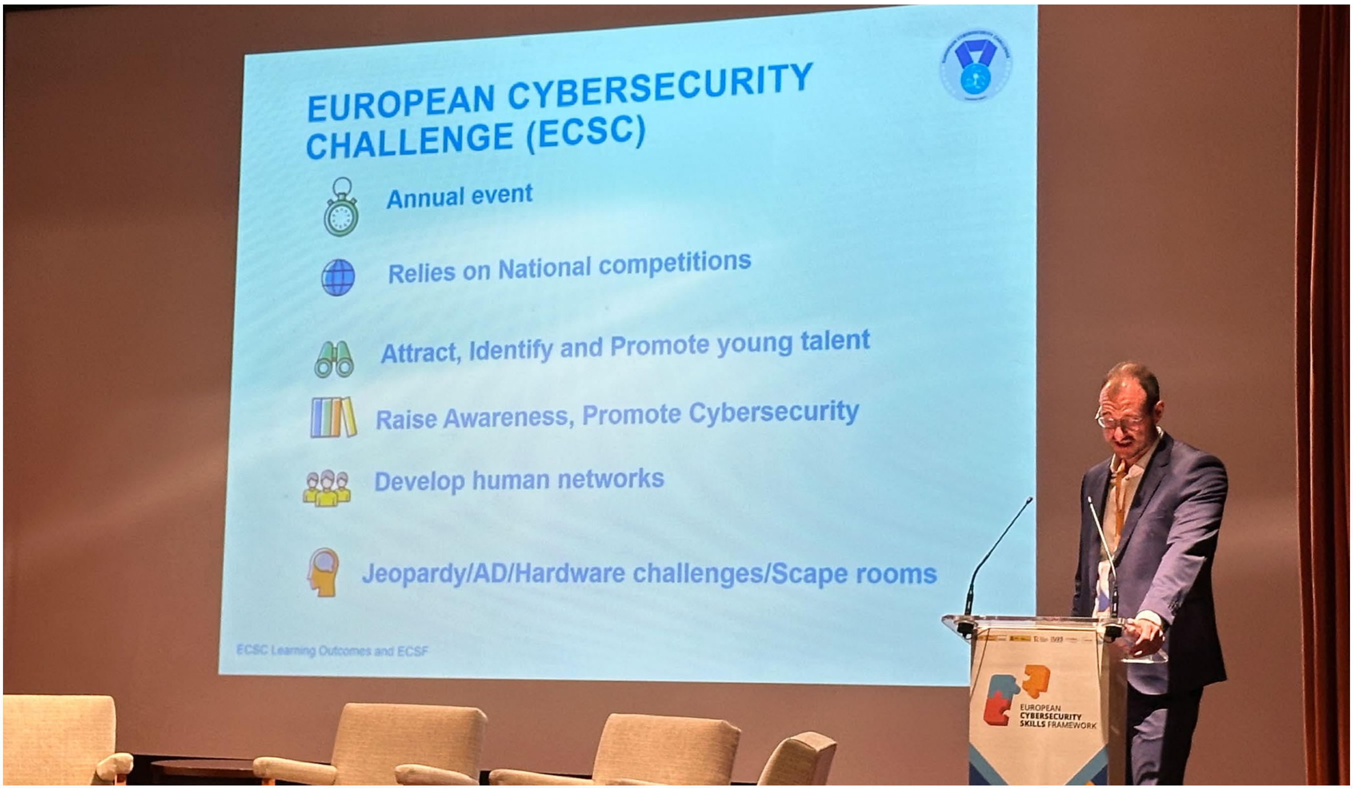
NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY

Unleashing America's Cyber Talent

JULY 31, 2023

OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE OFFICE OF THE PRESIDENT

Figure 6. Karen Wetzel, Manager of the Workforce Framework for Cybersecurity (NICE Framework) at NICE, presents the key priorities for developing America's cybersecurity workforce.



EUROPEAN CYBERSECURITY CHALLENGE (ECSC)

- Annual event
- Relies on National competitions
- Attract, Identify and Promote young talent
- Raise Awareness, Promote Cybersecurity
- Develop human networks
- Jeopardy/AD/Hardware challenges/Scape rooms

ECSC Learning Outcomes and ECSF

Figure 7. The European Cybersecurity Challenge is an initiative by the European Union Agency for Cybersecurity (ENISA) that aims to enhance cybersecurity talent across Europe and connect high-potential individuals with industry-leading organizations.

Figure 8. To promote economic advancement in regional Spain, the 2nd European Cybersecurity Skills Conference was held in Segovia, a historic city northwest of Madrid in central Spain's Castile and León region. To the right of the picture is the Alcazar of Segovia, a medieval castle that has existed since at least the 12th century.

3. EDTECH WEEK NYC 2023, New York City, USA

Attending EDTECH WEEK in New York City in October 2023 was a Fellowship highlight and a significant opportunity for the Fellow to advance their study on cybersecurity educational strategies and their alignment with sector demands. This conference provided an exceptional platform to explore the latest global educational innovations to reduce the digital skills gap. Interacting with renowned cybersecurity and educational technology figures, the Fellow engaged in meaningful conversations about effective teaching methodologies in the USA and the importance of collaborative efforts to prepare the future workforce to address new cyber threats.

The EDTECH WEEK event in NYC showcased an impressive lineup of speakers and workshops, including the Dean of the University of Pennsylvania Graduate School of Education and the Founder and Senior Science Advisor of Turnaround for Kids. The sessions focused on the latest trends in educational technology and practical strategies for implementing these innovations in different learning environments. Furthermore, workshops led by entrepreneurs and philanthropists provided valuable guidance on securing funding and building partnerships.

These discussions significantly enriched the Fellow's research by incorporating essential viewpoints and practical methods beneficial for establishing and implementing cybersecurity training programs in Australia. Moreover, the participation underscored the international dimension of the shortage in cybersecurity skills, highlighting the urgent need for enhanced global collaboration to address this challenge with the necessary determination and dedication.

The insights from EDTECH WEEK underscore the critical importance of international collaboration in addressing cybersecurity gaps within Australia’s vocational education sector. This collaboration offers a strong framework for enhancing educational programs and preparing students with the necessary skills to handle cybersecurity challenges.

The report strongly considers implementing strategic measures to improve vocational cybersecurity VET offerings. By drawing upon successful experiences from other countries, policymakers and industry leaders in Victoria can customise global insights to meet local needs. This adaptation process is essential to ensure strategies are tailored to Victoria’s unique digital economy requirements. Embracing this approach will help Victoria bridge the skills gap and establish itself as a leader in cybersecurity preparedness. This can be achieved by fostering a proficient, well-informed workforce capable of adapting to the demands of an ever-evolving digital environment.

Figure 9. EDTECH WEEK NYC 2023 was held at both the Times Centre NYC and one of Google’s NYC offices.

Figure 10. EDTECH WEEK NYC 2023 was held at both the Times Centre NYC and one of Google’s NYC offices.

08

The Impact of Interviews in Applied Research

Interviews with cybersecurity specialists have been pivotal in conducting applied research for this Fellowship. These discussions provided direct insights from industry leaders, offering a nuanced understanding of the current cybersecurity landscape and the existing skills gap.

Interviews play a vital role in applied research, allowing in-depth exploration of various topics (Guest, G, Namey, E and Mitchell, M., 2013). During these interviews, the Fellow engaged with top cybersecurity specialists worldwide, who generously shared their experiences, challenges, and considerations. These insights were invaluable for identifying and addressing the skills gap in cybersecurity. This method offers access to expert knowledge and practical insights often needing to be captured in quantitative data. This is particularly crucial in a field where threats and technologies evolve rapidly. The interviewed specialists, representing academia, industry and Government, highlighted critical areas where the skills gap is most pronounced. They emphasised the need for professionals proficient in emerging technologies and advanced threat detection methods. These discussions underscored the importance of aligning educational programs with industry needs to ensure graduates possess relevant, up-to-date skills.

Moreover, the interviews revealed systemic issues within the current vocational education framework, such as gaps in hands-on training and opportunities for real-world application of theoretical knowledge. This feedback is instrumental in enhancing curriculum design and training methodologies to better meet industry demands. Understanding the skills gap through these interviews also highlights broader implications for organisational security and resilience. A workforce needing more essential cybersecurity skills poses significant risks to data protection and digital infrastructure integrity. The research identifies specific skill sets in deficit and associated risks by engaging directly with industry experts.

The insights gained have practical implications for policy development and educational reform. Policymakers can create targeted initiatives to bridge the skills gap, while educational institutions can adjust curricula to better prepare students for cybersecurity challenges. This collaborative approach ensures that efforts to enhance cybersecurity education are grounded in industry realities, increasing their effectiveness and sustainability.

After conducting interviews with cybersecurity specialists, the Fellow has thoroughly shaped the strategy and considerations for closing Australia's cybersecurity skills gap. The qualitative data collected from these interviews will inform strategic considerations for improving cybersecurity education and workforce development to enhance Australia's cybersecurity capabilities.

09

Interviews conducted with cybersecurity specialists

The Fellow interviewed several prominent cybersecurity specialists to gain insights into the current landscape and address the skills shortage.

1. Dr Colin Soutar is a Managing Director at Deloitte & Touche LLP, where he leads Deloitte’s U.S. and Global quantum cyber readiness program. He is the GPS Cyber and Strategic Risk chief technology officer and leads the GPS Cyber Strategic Growth Offering. Before this role, Colin spent almost a decade as the chief technology officer for a Canadian-based biometric and identity management public company. His career began with a postdoctoral fellowship at NASA Johnson Space Centre, developing pattern recognition techniques for autonomous rendezvous and capture operations. He was part of the team that developed the 2013 National Institute of Standards and Technology (NIST) Cybersecurity Framework. He has helped NIST establish specific guidance for biometric technologies, identity, IoT, and privacy. Colin holds a PhD in computer science from the University of Strathclyde and a B.Sc. in computer science from the University of St. Andrews. The Fellow interviewed Colin in Washington, DC, where he shared his perspectives on the cybersecurity skills shortage and the needs of leading organisations. These insights have been invaluable in shaping the Fellow’s research direction and strategic considerations.
2. Marian Merritt is the Deputy Director and lead for industry engagement for the National Initiative for Cybersecurity Education, a program the National Institute of Standards and Technology (NIST) founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation’s oldest physical science laboratories. Congress established the agency to remove a significant challenge to U.S. industrial competitiveness at the time — a second-rate measurement infrastructure that lagged the capabilities of the United Kingdom, Germany and other economic rivals. Her focus areas include industry engagement, apprenticeship, and small business cybersecurity. With over 25 years in the cybersecurity industry, Marian previously worked with Symantec Corporation as their Director of Cyber Education and Online Safety Programs, where she created a cybersecurity career program for underserved young adults launched in 2014. Marian earned her undergraduate degree from Boston University’s Questrom School of Business and holds an MBA from the Wharton School at the University of Pennsylvania. The Fellow interviewed Marian in Venice, California.
3. Kristina Ishmael is the Deputy Director of the U.S. Department of Education’s Office of Educational Technology in the Biden-Harris Administration. She is crucial in developing national policies

on digital equity and AI in education, working closely with the White House and the Office of Science and Technology Policy. Significant reports were published during her tenure, including “Artificial Intelligence and the Future of Teaching & Learning.” The Fellow interviewed Kristina via Teams in Washington, DC, focusing on the critical role of STEM education in today’s digitally driven era. Kristina’s insights have influenced the Fellow’s research direction and strategic considerations.

4. Karen Wetzel, the Manager of the Workforce Framework for Cybersecurity (NICE Framework) at NICE, is a crucial figure within the National Institute for Standards and Technology (NIST) in the U.S. Department of Commerce. Joining the NICE team in October 2020, Karen has led efforts to develop, improve, and apply the NICE Workforce Framework for Cybersecurity to support an integrated cybersecurity education, training, and workforce development ecosystem. She specialises in community engagement and collaborates with stakeholders and subject matter experts to identify, communicate, and develop guidance, tools, and resources that address emerging trends and opportunities. The Fellow met with Karen in Segovia, Spain.

5. Laura Bernstein, a Principal within Deloitte’s Government Organisations Public Services Human Capital Practice, plays a pivotal role in developing human capital strategies. Her contributions significantly enhance the cybersecurity capabilities and robustness of public sector entities. The Fellow interviewed Laura via Zoom in Washington, DC, where she shared her perspectives on the cybersecurity skills shortage and the needs of many large U.S. Government organisations.

The information gathered from these interviews has been essential in shaping the direction of the Fellows’ research. The conversations around curriculum development, certification standards, and continual professional growth initiatives have provided valuable insights into critical aspects of cybersecurity education and workforce development. These discussions have given an essential understanding of the collaborative efforts needed to close the cybersecurity skills gap in Australia, which will serve as a solid foundation for guiding national initiatives in this vital area.

10

Strategies to Bridge the Skills Gap in Victoria - Six Considerations

A combination of interviews and conference attendance has proven a practical approach to applied research on the cybersecurity skills gap. This methodology provides a well-rounded perspective that integrates theoretical knowledge with valuable insights. The Fellow captured diverse viewpoints and up-to-date industry practices through this method, enriching the research findings. The synthesis of these comprehensive data sources has led to the development of seven key considerations. Each consideration is designed to address critical areas and drive meaningful improvements in closing the cybersecurity skills gap.

1. Graduate readiness for the cyber workforce

A comprehensive strategy integrating technical and non-technical skills development is essential to prepare cybersecurity graduates for the modern workforce adequately. This multifaceted approach is crucial due to the complexities of the current digital landscape, which require a skill set beyond what is typically taught in a vocational qualification.

Students must excel in network security and incident response areas and possess strong communication, problem-solving, and ethical decision-making abilities. These non-technical competencies enable them to collaborate effectively with interdisciplinary teams, communicate security issues to non-experts, and navigate the often complex ethical dilemmas associated with cybersecurity. By providing a well-rounded educational experience, vocational education institutions can ensure that their graduates are fully equipped to handle the challenges they will encounter in their professional careers. This will enhance their overall effectiveness and adaptability in the field.

Internationally, early intervention is critical. Programs designed for young students help build foundational cybersecurity skills. The Cybersecurity and Infrastructure Security Agency (CISA) emphasises starting education early to cultivate these essential skills. This presents an opportunity for Australia's VET sector to enhance its approach by incorporating cybersecurity education into school curricula. Adopting international best practices in this area could yield long-term advantages, significantly improving cybersecurity preparedness throughout the population.

It is crucial to equip graduates with the necessary skills to succeed in the rapidly evolving field of cybersecurity. VET can prepare a proficient workforce in cybersecurity by ensuring that current educational programs reflect the latest industry standards. This will enhance the employability of VET graduates and strengthen Australia's cybersecurity infrastructure. However, this requires significant resource investment, financial backing for new teaching methods, and updated materials. The payoff is clear: a well-prepared generation of graduates will strengthen Australia's cybersecurity infrastructure, keeping pace with global technological advancements and threats.

The VET sector can address the cybersecurity skills gap by hosting informational sessions on cybersecurity, encouraging student memberships in relevant associations, offering campus internships and mentorship programs, and including practical experiences like hackathons and simulated cyber-attacks to apply theoretical knowledge.

2. Empowering Women in Cybersecurity

To encourage girls and young women to pursue studies in cybersecurity, it's essential to implement specific strategies. First, it's crucial to promote female role models. Showcasing successful women in cybersecurity through school talks or media can help challenge gender stereotypes. During the Fellow's interview with Kristina Ishmael, the Deputy Director of the U.S. Department of Education's Office of Educational Technology, she emphasised the importance of the phrase "If you can see it, you can be it." She highlighted the diverse roles within the industry and the impact role models can have on girls' career choices. Integrating cybersecurity into school curriculums early is essential for building interest and foundational knowledge.

Also discussed in the interview were initiatives promoting women in cybersecurity, including several Government-led programs and strategies. The Cybersecurity and Infrastructure Security Agency (CISA) focuses on early education and exposure for girls, encouraging their participation in STEM programs to highlight the importance of cybersecurity. In 2023, the National Security Agency's National Centre of Academic Excellence in Cybersecurity (NCAE-C) released four grants to support related initiatives. The NSA invests directly in female talent by hosting rising junior and senior women from prominent cyber and STEM programs. Additionally, the NSA has improved its inclusive hiring strategy to benefit women in cybersecurity. Non-government organisations, like Women in Cybersecurity (WiCyS) and other groups, also strive to increase female representation in the field, aiming to foster a more inclusive and diverse cybersecurity workforce.

The United States has made significant strides within schools through initiatives like 'Girls Go CyberStart,' encouraging high school girls to explore cybersecurity (CyberStart America, 2021). While these school-based initiatives are valuable, it is essential to recognise the importance of early education. Several speakers at EdTech NYC highlighted the importance of teaching young children about cybersecurity. They stressed that educating children about online safety and privacy from a young age can prevent cybercrimes and protect personal information. Additionally, early cybersecurity education can open new career opportunities for teenagers who might not have considered this field.

Local competitions or clubs focused on cybersecurity for high school girls could be highly beneficial. However, securing funding and resources for these programs remains a challenge.

The benefits of these considerations include increased cybersecurity field diversity and potentially more innovative solutions due to varied perspectives. Potential obstacles consist of resistance from traditional educational institutions and societal stereotypes. However, the opportunities are vast, potentially empowering a new generation of women in cybersecurity. The threats involve the necessity for long-term commitment and funding for these initiatives. These strategies benefit organisations in the cybersecurity sector and promote gender equality in STEM fields. Access to a diverse talent pool with fresh perspectives enables significant progress toward a more inclusive future.

3. Cybersecurity Competitions

Hosting cybersecurity competitions for students can significantly enhance their readiness for the workforce. These contests provide a platform for students to apply theoretical knowledge in a practical setting, thereby improving their problem-solving capabilities and technical skills. They also offer exposure to real-world cybersecurity challenges, helping students understand the nature of threats and how to combat them effectively.

A central theme at the European Union Agency for Cybersecurity (ENISA) conference was the need for more practical initiatives to prepare the future workforce. Cybersecurity competitions at both local and national levels were highlighted as effective strategies. Local competitions allow for a wider reach and inclusion of students from various educational backgrounds, including those without access to traditional cybersecurity education. These events, organised by schools or universities with support from industry professionals and Government agencies, offer real-world scenarios for participants to tackle

Australian cybersecurity students are fortunate to have the opportunity to compete through the WorldSkills Australia Cyber Security Competitions, testing the skills and knowledge of over 4,000 apprentices, trainees, and students. Students compete for gold, silver, and bronze medals, with winners advancing nationally. The next rounds of regional competitions are underway on a two-year cycle, with national championships scheduled for 2023 and 2025.

These competitions align with the units of competency in the ICT50220 Diploma in Information Technology (Cyber Security specialisation). The regional events are team-based, with two competitors per team, and conducted virtually nationwide. Participants engage in various tasks to understand and implement attack and defence techniques, playing both roles to enhance their practical knowledge and skills. Functions in the regional competition, designed by Keysight Technologies, test competitors in key areas of cybersecurity. These include gathering, analysing, and interpreting threat data; protecting critical infrastructure; utilising design methodologies for security architecture; developing, implementing, and evaluating incident response plans; and reviewing and updating disaster recovery and contingency plans.

However, WorldSkills Australia Cyber Security Competitions are held every two years, meaning introducing more regular cybersecurity competitions within Victorian TAFEs could stimulate interest in cybersecurity careers and provide practical, more effective training opportunities than purely theoretical learning. Participation in regular competitions allows VET students to gain hands-on experience in identifying and addressing contemporary cyber threats while honing critical thinking skills. This practical training showcases and enhances participants' cybersecurity competencies effectively.

Organising cybersecurity competitions can be resource-intensive, but this challenge can be mitigated by engaging industry professionals. These experts can offer mentorship, judge competitions, and provide valuable networking opportunities for students. Ensuring these competitions stay current with the rapidly evolving cyber threat landscape is also crucial.

These competitions also bridge the gap between academic learning and real-world application, offering participants invaluable practical experience for their careers. By adopting such initiatives, the Victorian VET sector can better prepare students for the cybersecurity workforce and contribute significantly to enhancing overall cybersecurity readiness.

4. Introducing 'Externships' in the VET Sector

Introduced at EdTech NYC, 'Externships' gained significant momentum during COVID lockdowns by providing short, hands-on, remote work-based learning experiences. Unlike formal internships, 'Externships' allow students to explore organisations and career interests in a shorter, less formal setting. This helps students understand how their classroom learning applies in the real world and develop essential job-related skills.

In the United States, internships are seen as a critical component of work-based learning, complementing other career awareness activities (National Association of Colleges and Employers, 2023).

Compared to traditional placements or 'internships', work experience, and traineeships dominant in Victoria, externships provide more focused, hands-on experiences that could benefit the Victorian VET sector.

Introducing the 'Externships' model into Australia's VET sector could offer students flexible and diverse opportunities to gain industry exposure. This approach bridges the gap between theoretical knowledge and practical skills. A potential challenge is establishing enough business partnerships to support these opportunities. However, collaboration with industry professionals could mitigate this, ensuring externships are available in various fields.

The benefits of incorporating externships are significant. For educational institutions, this approach can enhance curriculum offerings and boost student engagement. Students gain unique industry exposure and practical skills, while businesses can identify potential employees and contribute to local talent development. These initiatives could result in a more skilled and prepared workforce in Victoria, benefiting the entire sector.

Externships also present investment opportunities. Discussions at the EdTech NYC 2023 conference highlighted growing interest in companies that offer externships or similar hands-on experiences for students. The return on investment includes financial gains and the development of a highly skilled workforce ready for the challenges of the digital age.

Partnerships with industry professionals are crucial to ensure that externships are valuable and relevant. These collaborations will align externships with industry needs, providing meaningful, practical experiences for students and preparing them for the demands of the future workforce.

5. Cybersecurity Capability Framework

The National Initiative for Cybersecurity Education (NICE) Framework, established by the National Institute of Standards and Technology (NIST), is crucial in helping large organisations manage their cybersecurity workforce planning effectively. This comprehensive framework provides organisations a structured approach to identifying, recruiting, developing, and retaining cybersecurity talent. The NICE Framework ensures that companies can systematically address their cybersecurity needs by categorising cybersecurity roles and defining the necessary skills, knowledge, and abilities. It facilitates alignment between workforce development and operational requirements, enabling businesses to build a competent cybersecurity team to tackle evolving threats and safeguard critical assets.

The NICE Framework can also provide a structure for the VET sector to prepare students for the cybersecurity workforce. The framework ensures that educational programs align with industry needs by categorising cybersecurity roles and defining the necessary skills, knowledge, and abilities. For the VET sector, this means developing curricula that address specific competencies required in the field, thereby enhancing the employability of their graduates.

Competency frameworks are used in the VET sector to define the essential skills, knowledge, and behaviours required for effective teaching. They are crucial in guiding curriculum development, evaluating teacher performance, informing professional development, improving student outcomes, and standardising teaching practices. By establishing clear benchmarks, these frameworks ensure that teachers are well-prepared to provide quality education and accommodate diverse learning needs, thereby fostering a consistent and high-quality teaching environment.

Integrating the NICE Framework into the vocational cybersecurity curriculum would allow the VET sector to develop structured courses covering key cybersecurity areas. Many educators are familiar with educational competency frameworks, and this organised approach helps instructors emphasise vital skills like threat analysis, incident response, and risk management. Moreover, the framework's distinct role definitions enable students to comprehend the different career paths within cybersecurity, empowering them to align their education with their career goals.

Furthermore, the NICE Framework facilitates partnerships between TAFEs and industry professionals, ensuring the training is relevant and current. These collaborations can include guest lectures, internships, and real-world projects that give students practical experience. Such initiatives enhance learning and help bridge the gap between academic knowledge and practical application, making graduates workforce-ready upon completing their studies.

Implementing the NICE Framework also helps Victorian TAFEs continuously assess and improve their cybersecurity programs. By regularly reviewing and updating course content to reflect the latest industry standards and emerging threats, TAFEs can maintain high-quality training that meets the evolving demands of the cybersecurity landscape. This ongoing alignment with the NICE Framework ensures that students receive a comprehensive and current education.

In summary, the NICE Framework equips Victorian TAFEs with a structured approach to preparing students for the cybersecurity workforce. Through well-defined roles and competencies, industry-aligned curricula, and continuous program assessment, TAFEs can effectively produce graduates ready to meet the challenges of modern cybersecurity environments.

6. Professional Cybersecurity Certifications in the Victorian TAFE Sector

Professional and academic cybersecurity certifications significantly enhance the readiness of graduates for the workforce. These programs provide structured learning that focuses on the practical application of theoretical knowledge. Earning a certification demonstrates an individual's competency in specific areas of cybersecurity, making them more attractive to potential employers. Certifications like the Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH) are widely recognised and valued. They validate a learner's expertise, increase earning potential, and open new career opportunities. Such credentials are highly regarded in the United States and have proven successful internationally.

There is growing interest in professional certification programs in Victoria, but the emphasis is less pronounced than in other regions. However, the success of these programs abroad suggests they could be highly beneficial within the Victorian VET sector. Integrating these certification programs into the Victorian TAFE system could provide students with a clear pathway to demonstrate their competencies and readiness for the cybersecurity workforce.

The strength of this approach lies in offering recognised credentials that employers value. A potential challenge is the cost associated with obtaining these certifications. To address this, partnerships with certification bodies could offer discounted exam vouchers or integrated certification pathways within the curriculum. Ensuring these certifications remain current with the rapidly evolving cyber threat landscape is crucial.

The benefits are substantial. For educational institutions, integrating certification programs can enhance curriculum offerings and boost student engagement. Students gain a richer learning experience that prepares them for their careers. For the cybersecurity industry, this means a workforce better equipped to tackle complex cybersecurity challenges. Overall, this strengthens Australia's cybersecurity defences, benefitting all stakeholders.

Sessions on cyber resilience, governance, and risk management underscore the need for professionals with a deep understanding of these areas, often demonstrated through professional certifications. The presence of expert speakers from various organisations, many of whom likely hold professional certifications, highlights their relevance and utility. Networking opportunities at conferences allow attendees to discuss the role and value of certifications with industry peers, further emphasising their importance.

By adopting these strategies, Victorian TAFEs can ensure that their graduates are well-prepared for the cybersecurity workforce and equipped with the theoretical knowledge and practical skills needed to succeed.

11

Impact of Bridging the Cybersecurity Skills Gap in Australia

The increasing demand for cybersecurity professionals in Australia has significantly improved employment prospects for graduates with cybersecurity qualifications at both vocational and degree levels. This demand is driven by the need to protect Australia's digital infrastructures from sophisticated cyber threats. The Federal Government's development of initiatives, such as the Cyber Security Strategy 2023-2030, has further increased these opportunities, positioning graduates favourably for employment in various sectors, including finance, healthcare, and government agencies. The increased need for cybersecurity professionals highlights the critical importance of a well-equipped and skilled workforce.

Australia's proactive approach to addressing cybersecurity challenges highlights the need for a comprehensive national plan to tackle the cybersecurity skills gap. Pillar Five of the Cybersecurity Strategy 2023-2030, which focuses on Sovereign Capabilities, aims to ensure Australia fosters a thriving cyber industry supported by a diverse and professional cyber workforce. Australia must invest in vocational education and training to consistently produce highly skilled cybersecurity graduates capable of effectively addressing current and future challenges.

This requires close collaboration between the VET sector and industry stakeholders. Aligning educational programs with industry requirements ensures relevant, hands-on training that equips graduates for real-world situations. This alignment contributes to developing a resilient and adaptable workforce capable of safeguarding digital assets across various sectors. These strategic initiatives position Australia as a leader in cybersecurity preparedness, protecting the nation's digital infrastructure and ensuring its resilience and security.

Insights from the cybersecurity sector can be applied to address skill shortages in other critical fields, such as aged care and early learning. Vocational education institutions must collaborate with industry stakeholders to design programs focusing on the required skills. This ensures graduates possess the competencies necessary to meet current demands effectively. Government, industry, and educational institutions working together can facilitate resource sharing, expertise, and best practices.

Almost immediately after graduation, ongoing professional development is also required to keep pace with the rapidly evolving cyber threat landscape. Continuous professional development (CPD) is essential in rapidly changing fields. This ensures cybersecurity professionals can handle new challenges. Implementing similar programs in other IT fields will help early career graduates stay updated with technological advancements, enhancing service quality and job satisfaction and retention. Leveraging technology, such as online platforms, simulation tools, and virtual reality, can also benefit the sector. This investment goes beyond technology, recognising the need for a cybersecurity workforce adept in technical, analytical and soft skills.

Government support is vital for addressing skill shortages. Policies incentivising vocational training and workforce development drive significant improvements. In cybersecurity, government initiatives have funded educational programs and fostered public-private partnerships. Similar policies in aged care and early learning could include grants for training programs, tax incentives for employers investing in staff development, and regulations standardising qualifications across the sector. Attracting talent to these fields requires clear, appealing career pathways.

More broadly, promoting career options in sectors affected by skills shortages, such as administrative positions and general leadership roles, can attract more candidates. The clear progression routes and potential for professional growth in these fields make them more attractive to prospective students. By focusing on these strategies, vocational education can build a competent and resilient workforce across various sectors, offering a promising future for those who choose these career paths.

In conclusion, successfully bridging the cybersecurity skills gap in Australia will positively impact employment prospects and highlight the importance of government and industry collaboration. These insights offer a blueprint for addressing skill shortages in other sectors, ensuring a well-prepared workforce for the demands of the modern economy.

12 Sector Engagement and Dissemination

Engaging with multiple stakeholders is vital for sharing the Fellow’s findings and considerations on addressing the cybersecurity skills gap. The Fellow has utilised various methods and platforms to share their insights, building strong partnerships with industry stakeholders, educational institutions, and Government bodies to guarantee that insights and strategies are widely disseminated and put into action. These efforts have been met with positive responses from all parties, resulting in increased awareness and action towards addressing the cybersecurity skills gap.

The Fellow has engaged with industry stakeholders through conferences, workshops, and webinars, allowing for open discussions about the current state of cybersecurity skills and potential solutions. The Fellow has gained valuable insights and feedback on their considerations by involving industry experts in these discussions. Early engagement and dissemination highlights include:

Vet Development Centre Thought Leadership Webinar: Bridging the Cybersecurity Skills Gap

The Vet Development Centre Thought Leadership Webinar: Bridging the Cybersecurity Skills Gap was successful. Over 730 registered participants attended the 90-minute webinar. Positive feedback included questions on gender imbalance, how to prepare graduates for the workplace, and how to incorporate soft skills into training packages.

The Fellow also used the webinar to articulate the opportunity the Fellowship offered to undertake applied research.

Friday, 26 July 2024, 12.00 pm - 1.30 pm AEST (11:30am ACST | 10:00am AWST)
Facilitator: Paul Goudie

The growing cybersecurity skills gap poses an increasing threat to Australia’s security and economic prosperity.

Join CEO of Altura Learning, Paul Goudie, for “Bridging the Cybersecurity Skills Gap.” This timely session will address the urgent need for skilled cybersecurity professionals and the crucial role of the Vocational Education and Training (VET) sector in filling this gap.

This presentation is a call to action for Australia’s VET sector, emphasising the national goal of becoming the leading cyber-secure nation by 2030. We’ll delve into the challenges within the current VET framework and propose strategies to enhance the quality and accessibility of cybersecurity education.

Topics covered include an overview of Australia’s cybersecurity skills gap, the role of the VET sector in cybersecurity education, challenges in the current VET framework, proposed strategies to address the skills gap, improving the quality of cybersecurity education, and future directions and action plans.

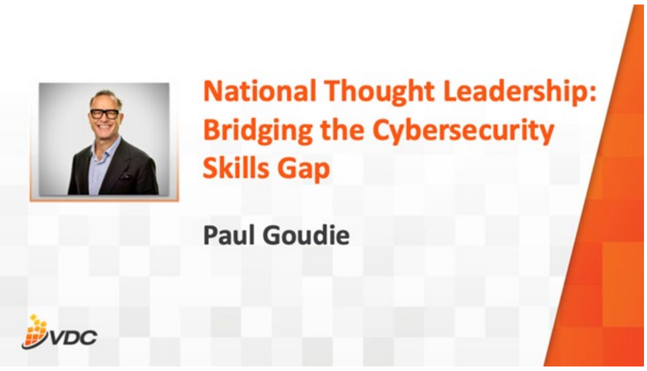
Participants will gain insights into cybersecurity skills' current and future needs, understand the VET sector's contributions and limitations, discover actionable strategies for improvement, and explore future goals and collaborative opportunities to advance Australia's cybersecurity capabilities.

Topics covered include:

- Overview of Australia's Cybersecurity Skills Gap
- Role of the VET Sector in Cybersecurity Education
- Challenges in the Current VET Framework
- Proposed Strategies to Address the Skills Gap
- Improving the Quality of Cybersecurity Education
- Future Directions and Action Plan

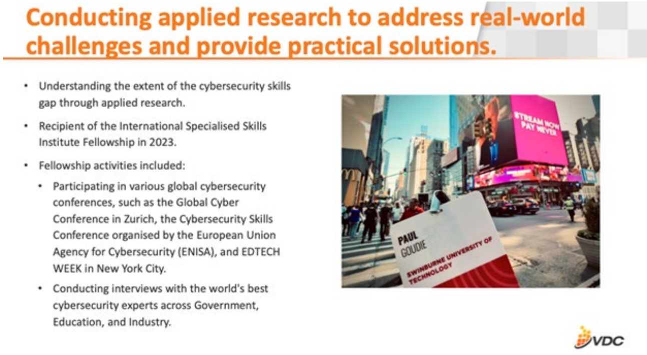
Audience

These sessions are for VET practitioners, educators, policymakers, RTO managers, CEOs and industry leaders.



National Thought Leadership: Bridging the Cybersecurity Skills Gap

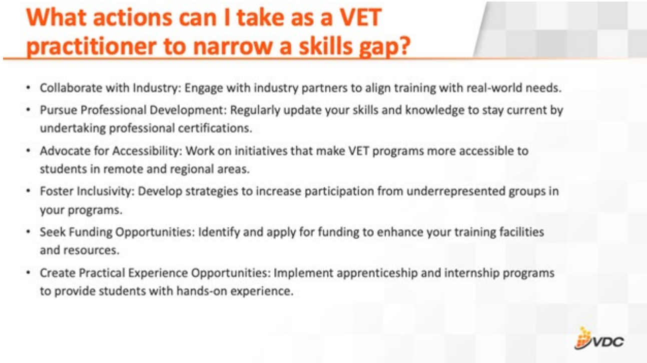
Paul Goudie



Conducting applied research to address real-world challenges and provide practical solutions.

- Understanding the extent of the cybersecurity skills gap through applied research.
- Recipient of the International Specialised Skills Institute Fellowship in 2023.
- Fellowship activities included:
  - Participating in various global cybersecurity conferences, such as the Global Cyber Conference in Zurich, the Cybersecurity Skills Conference organised by the European Union Agency for Cybersecurity (ENISA), and EDTECH WEEK in New York City.
  - Conducting interviews with the world's best cybersecurity experts across Government, Education, and Industry.

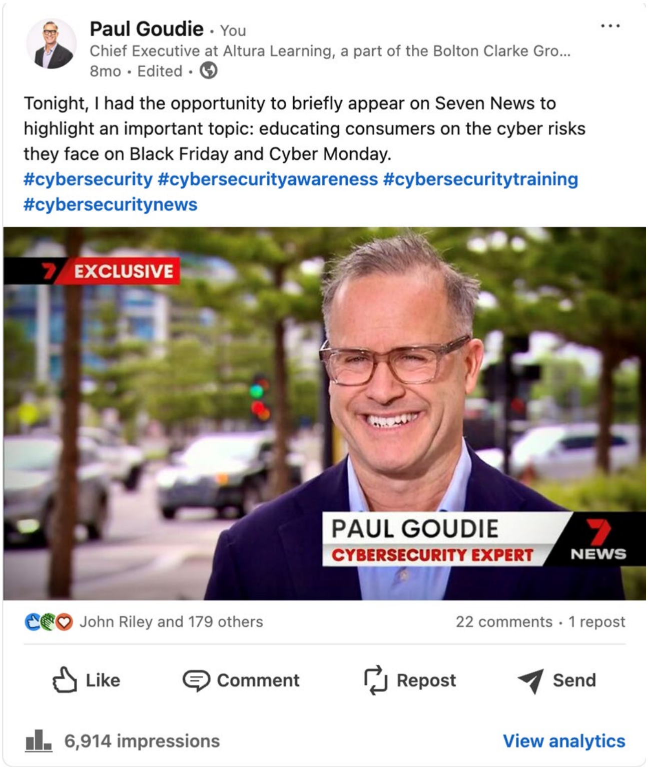
STREAM NOW
PAY NEVER
PAUL
GOUDIE
SWINBURNE UNIVERSITY OF TECHNOLOGY
VDC



What actions can I take as a VET practitioner to narrow a skills gap?

- Collaborate with Industry: Engage with industry partners to align training with real-world needs.
- Pursue Professional Development: Regularly update your skills and knowledge to stay current by undertaking professional certifications.
- Advocate for Accessibility: Work on initiatives that make VET programs more accessible to students in remote and regional areas.
- Foster Inclusivity: Develop strategies to increase participation from underrepresented groups in your programs.
- Seek Funding Opportunities: Identify and apply for funding to enhance your training facilities and resources.
- Create Practical Experience Opportunities: Implement apprenticeship and internship programs to provide students with hands-on experience.

Mainstream Media



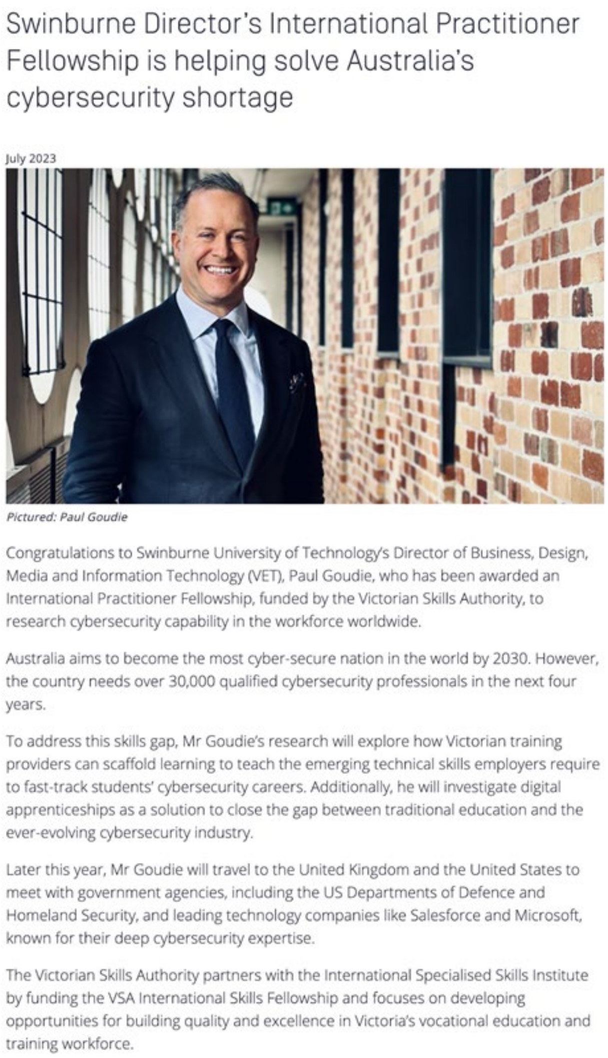
Paul Goudie • You
Chief Executive at Altura Learning, a part of the Bolton Clarke Gro...
8mo • Edited •

Tonight, I had the opportunity to briefly appear on Seven News to highlight an important topic: educating consumers on the cyber risks they face on Black Friday and Cyber Monday.
#cybersecurity #cybersecurityawareness #cybersecuritytraining #cybersecuritynews

John Riley and 179 others
22 comments • 1 repost

6,914 impressions
View analytics

Swinburne University’s External Communications



Swinburne Director’s International Practitioner Fellowship is helping solve Australia’s cybersecurity shortage

July 2023

Pictured: Paul Goudie

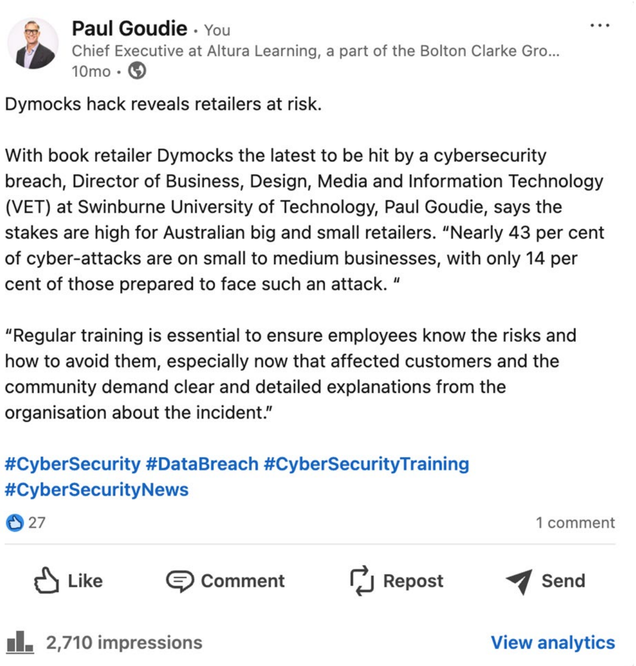
Congratulations to Swinburne University of Technology’s Director of Business, Design, Media and Information Technology (VET), Paul Goudie, who has been awarded an International Practitioner Fellowship, funded by the Victorian Skills Authority, to research cybersecurity capability in the workforce worldwide.

Australia aims to become the most cyber-secure nation in the world by 2030. However, the country needs over 30,000 qualified cybersecurity professionals in the next four years.

To address this skills gap, Mr Goudie’s research will explore how Victorian training providers can scaffold learning to teach the emerging technical skills employers require to fast-track students’ cybersecurity careers. Additionally, he will investigate digital apprenticeships as a solution to close the gap between traditional education and the ever-evolving cybersecurity industry.

Later this year, Mr Goudie will travel to the United Kingdom and the United States to meet with government agencies, including the US Departments of Defence and Homeland Security, and leading technology companies like Salesforce and Microsoft, known for their deep cybersecurity expertise.

The Victorian Skills Authority partners with the International Specialised Skills Institute by funding the VSA International Skills Fellowship and focuses on developing opportunities for building quality and excellence in Victoria’s vocational education and training workforce.



Paul Goudie · You
Chief Executive at Altura Learning, a part of the Bolton Clarke Gro...
10mo •

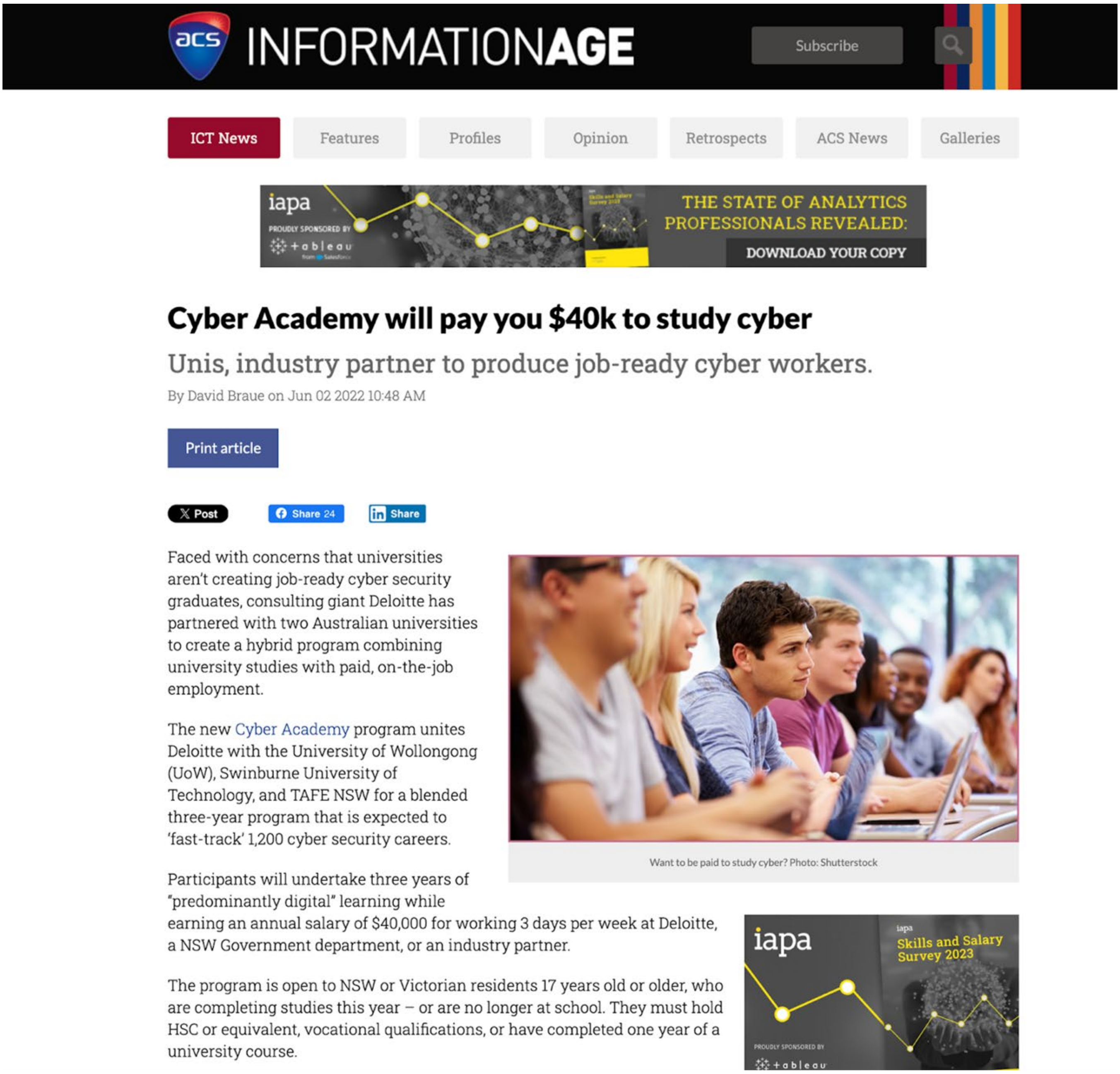
Dymocks hack reveals retailers at risk.

With book retailer Dymocks the latest to be hit by a cybersecurity breach, Director of Business, Design, Media and Information Technology (VET) at Swinburne University of Technology, Paul Goudie, says the stakes are high for Australian big and small retailers. “Nearly 43 per cent of cyber-attacks are on small to medium businesses, with only 14 per cent of those prepared to face such an attack. “

“Regular training is essential to ensure employees know the risks and how to avoid them, especially now that affected customers and the community demand clear and detailed explanations from the organisation about the incident.”

#CyberSecurity #DataBreach #CyberSecurityTraining #CyberSecurityNews

Curriculum Development: Cyber Academy, delivered at Swinburne University, TAFE NSW and the University of Wollongong.



Cyber Academy will pay you $40k to study cyber

Unis, industry partner to produce job-ready cyber workers.

By David Braue on Jun 02 2022 10:48 AM

Faced with concerns that universities aren't creating job-ready cyber security graduates, consulting giant Deloitte has partnered with two Australian universities to create a hybrid program combining university studies with paid, on-the-job employment.

The new Cyber Academy program unites Deloitte with the University of Wollongong (UoW), Swinburne University of Technology, and TAFE NSW for a blended three-year program that is expected to 'fast-track' 1,200 cyber security careers.

Want to be paid to study cyber? Photo: Shutterstock

Participants will undertake three years of "predominantly digital" learning while earning an annual salary of $40,000 for working 3 days per week at Deloitte, a NSW Government department, or an industry partner.

The program is open to NSW or Victorian residents 17 years old or older, who are completing studies this year – or are no longer at school. They must hold HSC or equivalent, vocational qualifications, or have completed one year of a university course.

13

Corresponding actions based on the stated personal goals

To enhance their expertise in cybersecurity, the Fellow has engaged with industry leaders following the return of travel and continued to immerse themselves in the latest trends, technologies, and methodologies. The strategy involves actively participating in discussions, workshops, and seminars to improve their understanding of cybersecurity. A highlight of this personal goal was hosting the VET Development Centre Thought Leadership Webinar "Bridging the Cybersecurity Skills Gap," which successfully attracted over 730 registered participants.

The invitation to represent Swinburne's Vice Chancellor at the VicScreen Digital Skills Round Table, hosted by Creative Industries Minister Steve Dimopoulos, was a crucial opportunity to contribute to thought leadership. It reflects the Fellow's significant contribution to cybersecurity discourse and contributes to the evolution of cybersecurity training packages, certifications, and micro-credentials.

The Fellow actively participated in developing courses at Swinburne University to tackle real-world cybersecurity challenges, emphasising technology. This hands-on approach allows for the seamless integration of theoretical knowledge into practical application, significantly improving the learning experience in Swinburne University's cybersecurity courses. Such active involvement is essential for creating an educational framework that is both engaging and effective.

At the same time, the Fellow has made it a priority to keep up their professional network. They have been reconnecting with global cybersecurity professionals whom they met during their Fellowship travels and participating in various networking events. The Fellow hopes these efforts will help them gain insights into international best practices. The main goal of these interactions is to expand their professional network and maintain these connections to stay updated with the latest advancements in cybersecurity education. The Fellow must continue these relationships after the Fellowship to keep their knowledge current and stay abreast of the latest developments in the field.

Corresponding actions based on the stated professional goals: A call to action for Australia's VET sector

The Fellow's research aimed to elevate the teaching of technical cybersecurity skills among Victorian training providers through a method known as scaffolding learning. This approach involved a comprehensive examination of current educational practices to pinpoint gaps and areas for improvement. The objective is to develop a practical model that VET providers could adopt, thereby enhancing students' employability in cybersecurity by offering clear guidance on addressing real-world challenges. In preparation for the recent intake of the Cyber Academy program, the Fellow thoroughly reviewed and updated the learning content against the Fellowship considerations. This process aimed to ensure that the curriculum reflected the latest advancements and methodologies in cybersecurity, enhancing the relevance and effectiveness of educational offerings.

Additionally, the Fellow investigated digital apprenticeships as a bridge between traditional education and the rapidly evolving demands of the cybersecurity sector. A primary focus of this initiative was how the concept of 'Externships' could be integrated into the curriculum. This integration prioritised equipping cybersecurity students with practical work experience, merging theoretical knowledge with real-world application. The 'Externship' concept emphasises practical skills and experience and provides students with a clear pathway to employment. Vocational programs benefited from direct industry engagement, enabling students to gain hands-on experience and build professional networks before graduation. It's critical to foster collaborations between TAFE institutions and employers on an ongoing basis to facilitate a suitable pool of employers who can provide the 'Externship' opportunity and assist with the transition of newly qualified professionals into the cybersecurity workforce.

International collaboration was a vital component of the Fellow's research. By meeting with government bodies, technology firms, and academic institutions in the U.K. and the U.S., the Fellow sought to learn from their practical approaches to cybersecurity education. This international collaboration provided valuable insights and best practices that have been incorporated into the Australian cybersecurity education system. This ensures students have the necessary skills and experience to excel in this fast-evolving industry. The work being led in the U.S. in advocating for greater diversity within the cybersecurity industry is imperative. Efforts are focused on attracting and retaining talent from underrepresented communities through diversity and inclusion initiatives, informational sessions, and creating supportive networks.

The aim is to make a lasting impact on the cybersecurity landscape. The Fellow intends to establish a long-term strategic vision for the sector through fellowship activities and sustained advocacy. This involves continuously assessing and refining current practices and maintaining active engagement with the industry to contribute to the enduring advancement of cybersecurity.

By pursuing these goals, Australia's VET sector, a crucial player, can significantly contribute to preparing a skilled and diverse cybersecurity workforce ready to meet industry demands.

14 Conclusion

In summary, the combined efforts of Australia's VET sector offer significant promise in addressing the cybersecurity skills gap and positioning Australia as a global leader in cybersecurity by 2030.

The thorough analysis presented in this report emphasises the importance of addressing current shortcomings through curriculum reforms, collaboration between the VET sector and industry, and improved teacher currency. By nurturing solid educational-industry partnerships, the VET sector can produce a workforce capable of tackling existing cybersecurity threats and adapting to the changing demands of the digital landscape.

The Fellows' involvement in international conferences and extensive research has highlighted the crucial role of continuous professional development and lifelong learning in establishing a dynamic and responsive cybersecurity education framework. Initiatives such as the Free TAFE and promoting digital inclusion are commendable steps towards cultivating a skilled and inclusive cybersecurity workforce.

The strategic interventions proposed in this report aim to enhance the quality and accessibility of cybersecurity education within Victoria. By implementing these measures, Victoria significantly strengthens its cybersecurity defences, safeguarding its digital future and setting a benchmark for other regions. Collaboration between Government, industry, and educational institutions is essential for ensuring that Victoria remains resilient and adaptable in an ever-changing cybersecurity landscape.

15 References

Hong, C., 2022. The case for applied degree education: The future of learning for the new world of work. In Applied degree education and the future of learning (pp. 1-25). Singapore: Springer Nature Singapore.

Australian Government, 2023. Australia's Cyber Security Strategy 2023-2030. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

NCVER, 2023. VET Student Outcomes 2023. https://www.ncver.edu.au/__data/assets/pdf_file/0044/9684593/VET_student_outcomes_2023.pdf

European Training Foundation, 2024. Making the Case for Vocational Education and Training Improvement: Issues and Challenges. https://www.etf.europa.eu/sites/default/files/m/270970490A6E9327C1257CA800407038_Quality%20assurance%20in%20VET.pdf#page=5

Victorian Government, 2021. Victorian Digital Strategy 2021. https://content.vic.gov.au/sites/default/files/2022-02/DPC_Vic%20Gov%20Digital%20Strategy%202021-26_Accessible_V11.1_updated%20Feb%208.pdf

Guest, G., Namey, E.E. and Mitchell, M.L., 2013. Collecting qualitative data: A field manual for applied research. Sage.

National Institute of Standards and Technology (NIST), 2020. NICE Cybersecurity Workforce Framework. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

CyberStart America, 2021. Girls Go CyberStart Initiative. https://www.girlsgocyberstart.org

National Association of Colleges and Employers (NACE), 2018. Internships and Work-Based Learning. https://naceweb.org/career-readiness/internships/students-internships-positively-impact-competencies/

International
Specialised
Skills
Institute

est. 1991