Digital skills and cyber security: How do we secure our future?

RMIT Blockchain Innovation Hub

RMIT Centre for Cyber Security Research & Innovation

RMIT Digital Ethnography Research Centre

RMIT UNIVERSITY

Published by:

RMIT Blockchain Innovation Hub

RMIT UNIVERSITY Centre for Cyber Security Research and Innovation

digital ethnography research centre

Authors:

Dr Ahmad Salehi Shahraki, Dr Konrad Peszynski, Dr Banya Barua, Laki Kondylas and Amarens Breteler.

Acknowledgments:

Thank you to the Digital CBD Project team, the RMIT Centre for Cyber Security Research & Innovation and the RMIT Blockchain Innovation Hub, especially Professor Matt Warren, Distinguished Professor Jason Potts and Associate Professor Chris Berg for their help with the ideation and production of this report.

Published: July 2022

Contents

Authors 2

Foreword 4

Executive Summary 5

Introduction 7

Background 10

Melbourne’s smart city’s credentials 12

Melbourne’s Digital CBD 13

Melbourne as a Digital CBD through a human lens 15

Defining digital skills 20

Information, communication and technology skills 21

Cyber security skills 22

Developing digital skills through education 22

Victoria’s digital skill responses during COVID-19 23

The impact of COVID-19 24

Increased digitalisation 25

Zero migration 26

Increased cyber threats 26

The shortage of digital skills in Australia 27

Melbourne Digital Skills Survey 2022 28

Effect of COVID-19 on Melbourne’s digital professionals 29

How the working arrangements of digital professionals were affected 30

Digital technologies and digital skills 31

Significant investment in new technologies, but is it enough? 32

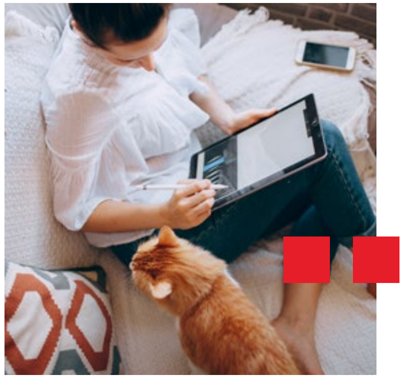
How are organisations placed in terms of the digital skills of their employees? 33

Cyber security skills 34

Role of individuals and industry in training and qualifications 36

What role does the industry play? 37

Recommendations 38



Foreword

from Director Professor Matt Warren

Professor Matt Warren

It is my distinct pleasure to introduce this report, the fourth in a series of five – 'Digital skills and cyber security: How do we secure our future?'. This report will examine the current digital skills gaps in Melbourne's labour market. An important first step on the path toward global excellence, for the state of Victoria.

For Melbourne to become a Digital Central Business District (CBD), we need to enhance our collective understanding of the digital skills shortages among professionals – which is why the authors of this report conducted in-depth research that aims to shine a light on this issue.

This report will focus on the ways we can enhance the innovation of public and private organisations by identifying the areas of opportunity in the digital skills landscape. Ensuring Melbourne transforms into a digital leader for cities around the world is a thrilling aspiration. We are proud to offer our services to help shape Melbourne's future, its CBD and the broader regional economy in the aftermath of the COVID-19 pandemic.

As the COVID-19 pandemic unfolded, most of us started working and studying from home. This shift advanced the need for rapid digitalisation, which resulted in an increased dependency on advanced technologies.

On the one hand, the people of Melbourne have shown immense grit and resilience by adapting to these changes, and rising to numerous other challenges that the pandemic brought about. Indeed, the effects of the pandemic were so profound that hardly any aspects of life remained untouched by it. However, the way Melbourne bounced back after being in lockdown for longer than anywhere else on the planet truly shows our collective buoyancy as a city, and as a community.

On the other hand, our increased dependency on technology also functions as a catalyst for cyber security threats. Despite our public-spirited resilience, we are more vulnerable than ever to cyber security attacks as the new environments we study and work in demand unprecedented agility and precaution from us.

There was already a profound shortage in cyber security skills, which the pandemic has only perpetuated. Therefore, it is imperative for both employers and employees to develop the appropriate digital skillset for the future.

In this ground-breaking report, the authors identify current digital skills gaps and provide a course of action for Melbourne to become a secure and successful Digital CBD - so that we can become a global tech leader and set an example for cities all over the world.

At RMIT University, we are thoroughly excited to be playing a key role in the reinvention of Melbourne's CBD as a hybrid and dynamic digital playground.

Professor Matt Warren

Director RMIT Centre for Cyber Security
Research and Innovation

Executive Summary

This report investigates the impacts of the rapid development of technologies and the effect of the COVID-19 pandemic (known as the twin shocks) on the digital skills shortages in the Victorian labour market. Specifically, it attempts to understand the current digital skills issues, and the challenges the pandemic brought about, in the context of developing Melbourne as a Digital CBD.

The global events of the last two years have sped up the adoption of digital technologies by several years[1]. Companies are rethinking the role of digital technology and how it is impacting the ability to conduct business at a rapid pace.

As indicated in the first report of this Digital CBD series, Melbourne is the perfect case study for the development of a Digital CBD. It is a dynamic and inventive city with creative and talented people at its core.[2]

Given that we are still living in the aftermath of the pandemic, now is the time to 'reset' Melbourne, and build upon its unique strengths and foster a thriving, connected and responsive city: a Digital CBD. Such a Digital CBD, however, would become unsustainable if Melbourne's people lacked the appropriate digital and cyber security skills that make the city resilient and prepared for future challenges.

Currently, there are significant ICT (information and communication technology)[3] skills gaps and shortages that are highly problematic, as they threaten our national security.[4,5,6,7]

The gaps between know-how, practical experiences, and the specific skills needed for the knowledge economy of 2022, represent a poignant issue for the future of Australia's domestic and international economic development – particularly when analysed through a COVID-19 lens.

Therefore, it is fundamental that the issues described above are thoroughly investigated if we want to safeguard our national security from cyber threats.[8]

The global events of the last two years have sped up the adoption of digital technologies by several years.

[1] The new digital edge: Rethinking strategy for the post pandemic era
[2] Digital CBD Project Report 1
[3] The ACSC Essential 8
[4] ACSC Annual Cyber Threat Report - 1 July 2020 to 30 June 2021
[5] NCVER Generic skills in VE and training
[6] ACDS Benchmarking
[7] K4D Emerging Issues Report
[8] Gilbert & Tobin Victoria's Cyber Security Strategy 2021

In Victoria, there is a need for enhanced digital skills that are in lockstep with the technology, applications and management of the Digital CBD. Such improved skills could make Melbourne one of the most digitally connected cities in the world.

However, emerging technologies are creating a considerable number of cyber security challenges, competitiveness and resilience.

Melbourne Digital Skills Survey 2022 Fast Facts:

88%

of respondents indicated that **COVID-19 had changed the way their organisation undertook their business.**

85%

of respondents indicated they would like to **continue working from home in some capacity.**

45%

of respondents indicated that **their organisation does not have the digital skills that they require.**

70%

of respondents indicated **they do not have enough staff dedicated to cyber security and that there is a shortage of digital skills in their organisation.**

70%

of respondents felt that **COVID-19 has left them more susceptible to cyber threats.**

This report aims to identify the most sought-after digital skills in the Victorian labour market, and the existing areas of opportunity for the development of such skills. Based on research findings, and an analysis of the Melbourne Digital Skills Survey 2022, this report will provide practical recommendations to the public and private sectors to close the existing digital skills gap.

Recommendations include:

1. **Establishing a Victorian Digital Skills Academy.**
2. **Establishing an Australian Cyber Security Accreditation Body and an Australian Cyber Security Body of Knowledge.**
3. **Creating a comprehensive ICT and Cyber Security Diversity Action Plan for Victoria.**
4. **Increasing skilled migration to aid Victoria's recovery.**
5. **Investing in innovative school programs highlighting the skills required in a digital economy.**
6. **Creating a program to increase the awareness of digital technologies and the need to upskill digital skills within the Melbourne CBD.**

Introduction

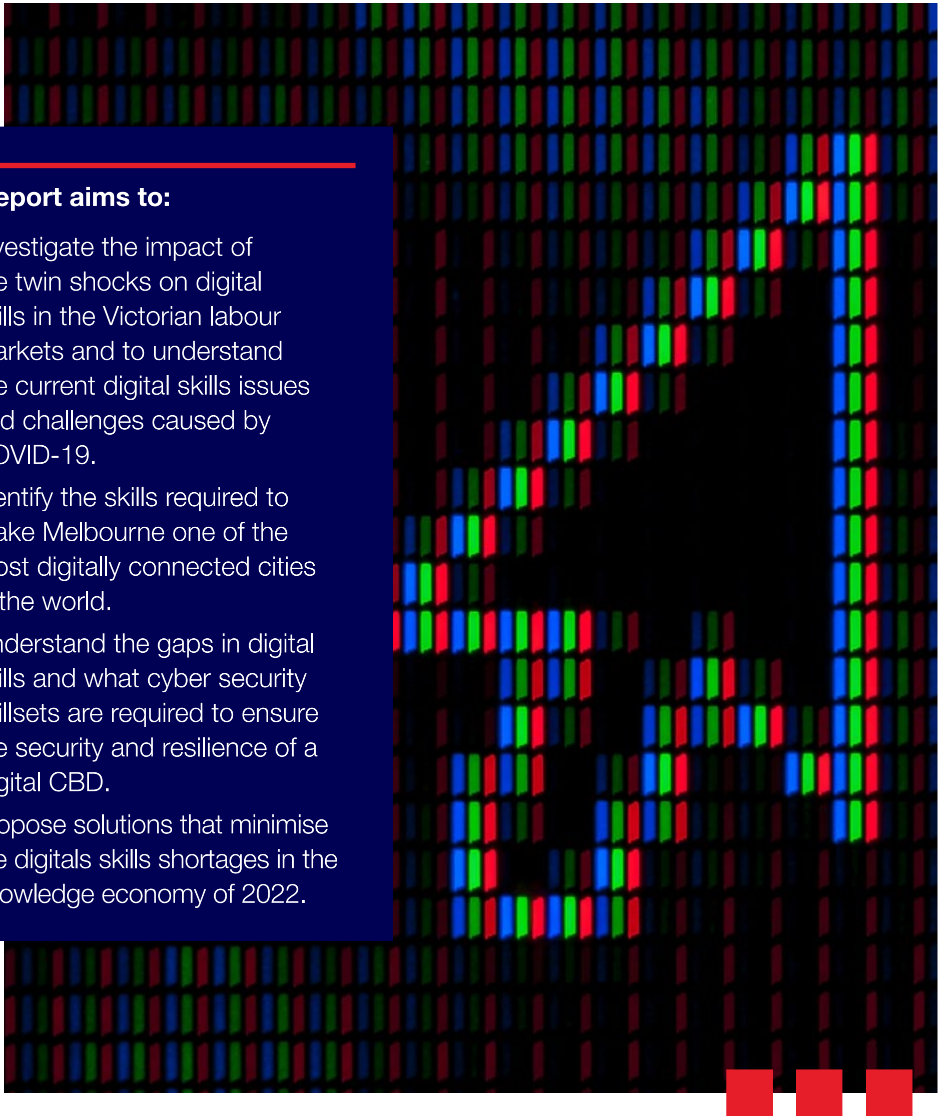
Introduction

This report investigates the impact of the twin shocks on digital skills shortages and the Victorian labour market. Specifically, it attempts to gain a better understanding of the current digital skills issues, and the challenges the COVID-19 pandemic posed to the development of a Digital CBD.

Prior to the pandemic, many organisations were trying to understand the impact of the accelerated automation of jobs. Such as the adoption of Artificial Intelligence (AI), the embedding of analytics into business processes and the proliferation of remote work. These were some of the technology-driven trends that were altering the nature of work and skills.[9]

If anything, COVID-19 illuminated the cracks in the ways businesses were ran. Now, many organisations are investing heavily in technology to address pandemic-induced problems, such as interrupted supply chains and failing revenue.[10]

While technology is an important component of digital transformations, it doesn't solve all problems. In fact, Sundar Pichai, the Chief Executive Officer of Alphabet and its subsidiary Google stated that "*technology doesn't solve humanity's problems. It was always naive to think so.*"[11]



This report aims to:

- Investigate the impact of the twin shocks on digital skills in the Victorian labour markets and to understand the current digital skills issues and challenges caused by COVID-19.
- Identify the skills required to make Melbourne one of the most digitally connected cities in the world.
- Understand the gaps in digital skills and what cyber security skillsets are required to ensure the security and resilience of a Digital CBD.
- Propose solutions that minimise the digitals skills shortages in the knowledge economy of 2022.

[9] Guterman Z 2022 'Fixing the digital skills gaps in the post COVID-19 workplace' 16 July 2022

[10] McKinsey & Company 2020 - How COVID-19 has pushed companies over the technology tipping point

[11] The New York Times Sundar Pichai of Google: 'Technology Doesn't Solve Humanity's Problems'

Businesses need to develop a better understanding of the digital skills labour market, the types of roles, certifications and qualifications required.

> "The twin shocks of COVID-19 and rapidly accelerated technology adoption have impacted workplaces, work practices, supply chains and the wider economy - as well as radically changing our day-to-day experiences. The COVID-19 pandemic, and the associated lockdowns immobilising the public and businesses, has prompted the radical restructuring of economic activity and forced rapid digital adoption. As a result, companies may no longer look the same, and many may never return to a pre-COVID status quo."[12]

The World Economic Forum indicated that a large skills gap would remain as in-demand skills across jobs change in the next five years.[13] As such, businesses need to develop a better understanding of the digital skills labour market, the types of roles, certifications and qualifications required. As well as the skills shortages and gaps to be addressed to ensure Melbourne's CBD transforms into a digital leader for cities around the world.

To help us develop insight into the current prevailing skills gaps in Melbourne's CBD, we conducted a survey that was targeted at digital technology professionals in the ICT and cyber security sectors.

These professionals often experience a shortage of digital and cyber security skills first-hand. They also possess specific industry knowledge that helped identify solutions to the problem.

[12] Digital CBD Project Report 1 (n 2)
[13] World Economic Forum The Future of Jobs Report 2020

Background

The RMIT Blockchain Innovation Hub[14], RMIT's Centre for Cyber Security Research and Innovation[15] and the Digital Ethnography Research Centre[16], have come together to conduct large-scale research and have produced a series of reports that consider the acceleration of digital technology, directly impacted by COVID-19, and consequently, the areas of opportunity for a Digital CBD.

The Digital CBD project reports aim to provide a strategic roadmap for the creation of a Digital CBD[17]:

Report 1 - 'The future of the Digital CBD: Melbourne and beyond' was released in December 2021 and set the vision for building a Digital CBD in Melbourne. It identified Melbourne as an ideal case study for a Digital CBD due to its dynamic and world-leading reputation combined with innovative and talented people.

Report 2 - 'The Docklands DAO: Reimagining precincts in a Digital CBD', proposed building a new type of digital economic infrastructure: a DAO (Decentralised Autonomous Organisation) that could create a new local resource for city data and develop a new model for community participation.

Report 3 - 'Towards just and resilient supply chains for the Digital CBD', explored the utilisation of innovative emerging technologies such as blockchain technology, AI, Machine Learning (ML) and the Internet of Things (IoT) as well as their applications to address the supply chain challenges and cyber security risks within the context of a CBD.

[14] RMIT Blockchain Innovation Hub
[15] RMIT Centre for Cyber Security Research and Innovation
[16] RMIT Digital Ethnography Research Centre
[17] Digital CBD Project Reports

This current report, Report 4 – 'Digital skills and cyber security – securing our future' – focuses on the digital skills gap that we are experiencing, which is a risk for a future Digital CBD.

And finally, to complete the Digital CBD roadmap, **Report 5 – 'Are people ready for a Digital CBD? The new infrastructure demands required'** explores the infrastructure requirements needed to make the shift to a fully integrated digital city that includes businesses, culture, physical space and of course - people.

Given that technology is an enabler and one part of the digital transformation puzzle, many difficult questions are raised about the broader impact on jobs, skills, wages and the nature of work itself.[18] This report seeks to shine light on this issue.

Ensuring we have the right digital and cyber skills is critical if we want to build a truly sustainable Digital CBD. To gain a thorough understanding of the impacts of COVID-19 on Melbourne, we need to go back in time.

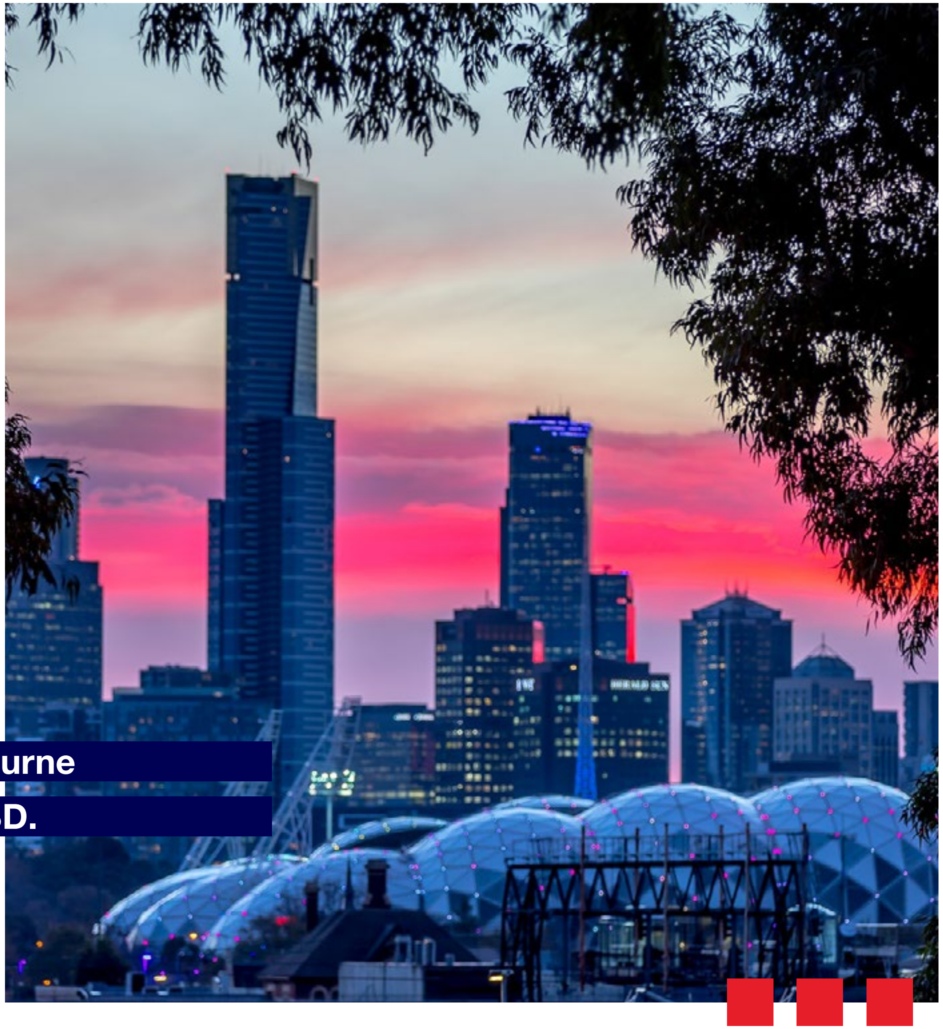
[18] McKinsey & Company 'Technology, jobs, and the future of work' 24 March 2017

Melbourne's smart city's credentials

Prior to the pandemic, Melbourne was ticking all the smart-city boxes.

- ☑ Melbourne was ranked in the top three cities globally for technology, top five for data and analytics, top five for cyber security and top four for connected citizens.[19]
- ☑ Melbourne placed 13th among 100 cities globally in terms of its talent availability.[20]
- ☑ Australia ranked sixth out of 50 countries when assessed on digital criteria on the Tholons Global Innovation Index 2021.
- ☑ Melbourne was one of the top-ranked cities for digital skills according to according to the 2021 World Best Cities report.[21]
- ☑ The 2021 Global Talent Competitiveness Index reported that Melbourne was one of the top cities globally that attracted top-tier talent and is growing rapidly in the areas of education, environmental quality, safety and airport connectivity.[22]
- ☑ 37 of the world's top universities are located in Australia with more than five of them located in Melbourne. Based on analysed data by Times Higher Education, our universities are attracting the highest number of international students after the UK and the US.[23]
- ☑ Melbourne was one of the top-six cities globally for students.[24] This was based on factors such as affordability, desirability and the options for existing students.

Strong smart-city credentials set Melbourne up to become a worldleading Digital CBD.



[19] ESI Thoughtlab 'Building a hyperconnected city'
[20] Tholons 'Tholons released 2021 Global Innovation Index'
[21] Resonance Consultancy World's Best Cities Report 2021
[22] The Global Talent Competitiveness Index 2021 Accenture
[23] The Student – Discover best universities
[24] QS Best Student Cities Rankings 2022 | Top Universities

Melbourne's Digital CBD

But what is a Digital CBD?

A Digital CBD is a complex ecosystem of private and public services and entities, people, devices and digital infrastructure that continuously interact with each other.

Digital CBD technology includes several layers where data is generated, processed, stored and transferred over millions of devices, applications and platforms. This enormous data value is always transmitted and freely distributed over open networks, increasing the chances of new cyber threats and attacks.[25]

Australia's cities generate 80% of the national GDP. Embracing new technology will revolutionise how cities are planned, function and how the economy grows.[26]

New technologies such as AI, ML, IoT and blockchain are classified as critical technologies, which have the capacity to significantly enhance or pose risk to our national interests. They are fundamental to Australia's economic prosperity, social cohesion, national security, and are increasingly the focus of international geopolitical competition.[27]

Melbourne is one of the most liveable cities on the planet and has been for the last seven years, according to Economist Intelligence Unit.[28]

Cities like Melbourne play a unique role in the economic recovery from the pandemic as most of the world's people live and work in urban conglomerates. It has been predicted by the United Nations (UN) that by 2050, 68% of the worls population will be living in a city.[29]

Predictions like this indicate that Melbourne will have to ready itself for increased population growth. Parallel to such changes are new challenges that demand a new set of competencies.

[25] Digital CBD Project Report 1 (n 2)
[26] Smart Cities Plan – Australian Government
[27] The Action Plan for Critical Technologies – Australian Government
[28] Wahlquist C 2017 'Melbourne world's most liveable city for seventh year running' The Guardian
[29] United Nations (2018), Department of Economic and Social Affairs Population Dynamics: World Urbanization Prospects 2018, New York: United Nations,.

Smart cities

Technology plays a key role in urban areas that use different types of electronic methods to collect specific data, these areas are also known as ‘smart cities’. Melbourne is one of these smart cities, in which people utilise technology daily, meaning that they need to be cyber-savvy to meet the demands of the current knowledge economy.

Specifically, technology is intertwined with organisational characteristics and capabilities as these factors influence technology enactment.[30]

Technology enactment encompasses the impact of behavioural patterns; micro and macro-level institutional factors such as norms, values, perceptions, rules, routines, practices and regulations; that shape the way information and communication technologies are applied in various organisations.[31]

Each day, Melburnians rely on the services provided as critical infrastructure such as:

- Communications
- Financial services and markets
- Data storage or processing
- Defence industry
- Higher education and research
- Energy
- Food and grocery
- Health care and medical
- Space technology
- Transport
- Water and sewerage

Industry 4.0

Where Industry 3.0 was all about moving from mechanical and analog processes to digital ones, Industry 4.0[32] is defined by rapid changes to technology due to increasing interconnectivity and smart automation. Thus, Industry 4.0 is all about making business smarter and more automated.

Examples of Industry 4.0 technologies include:

- Big data and analytics
- Autonomous robots
- Digital twins
- IoT
- Cyber security technology
- The Cloud
- AI
- Augmented reality

[30] Faro, B., Abedin, B., & Cetindamar, D. (2021). Hybrid organizational forms in public sector’s digital transformation: a technology enactment approach. Journal of Enterprise Information Management

[31] Mu, R., Haershan, M., & Wu, P. (2022). What organizational conditions, in combination, drive technology enactment in government-led smart city projects? Technological Forecasting & Social Change, 174, 121220–.

[32] Immerman, G, 2020 ‘Emerging Industry 4.0 technologies with real world examples

Melbourne as a digital CBD through a human lens

For any technology to be adopted and adapted, three essential factors are considered vital:

- Humans
- Processes
- Technology

The pandemic and its outcomes accelerated the role of technology, both in the workplace and at home. COVID-19 has made technology an integral part of human life.

People are an indispensable part of technology development and implementation.

The people of a city play critical roles in the adoption of technology and these are the following:

- Administrators
- Organisers
- Developers
- End-users

Advanced technologies, especially those related to critical digital infrastructures, become much more significant to people as they directly impact their lives.

The adoption of critical digital infrastructure is still nascent, while the need for advanced technologies has considerably increased – especially post-pandemic. Therefore, a widening gap is emerging between technology and people which is explored in the fifth report of this Digital CBD research series: **'Report 5 - Are people ready for a Digital CBD? The new infrastructure demands required'**

The unique relationship between people and technology

Working with and applying advanced technologies requires certain behaviours from people who use them. These behaviours could be a blend of cognitive skills such as thinking and reasoning as well as non-cognitive skills such as motivation, integrity and interpersonal interaction.[33] Although today's advanced technologies have enormous benefits, they are also closely associated with risks. These risks include the ability of hackers to manipulate users' perceptions, influence their behaviour, and rely on these actions to carry out a cyber attack[34]. These attacks are carried out through the delivery of misinformation via various media platforms, such as email. Here, the impression of a trusted source is often created.[35]

[33] Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: abundant opportunities for research at the interface. Journal of Business and Psychology, 37(1), 1–29.

[34] Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. Frontiers in Psychology, 12, 561011–561011

People are an important part of the exploration and implementation of Industry 4.0 and Web3.

Phishing is an example of a cyber attack.

Attackers send seemingly innocuous e-mails to targeted users, inviting them to divulge protected information for apparently legitimate purposes. This is similar to the nefarious practice called 'baiting', in which malware-infected software is left in a public place in the hope that a target user will find and install it, thereby compromising the entire computer system.[36]

Phishing accounts for around 90% of data breaches according to the CISCO 2021 Cyber security Threat Trends Report.[37]

To manage the intensity of technology advancement in Industry 4.0, it is crucial that people can assess the trustworthiness of interactions and are able to remain unbiased in the perception of a threat. Digital transformation is often problematic as unlearning and relearning certain behaviours are challenging processes.[38]

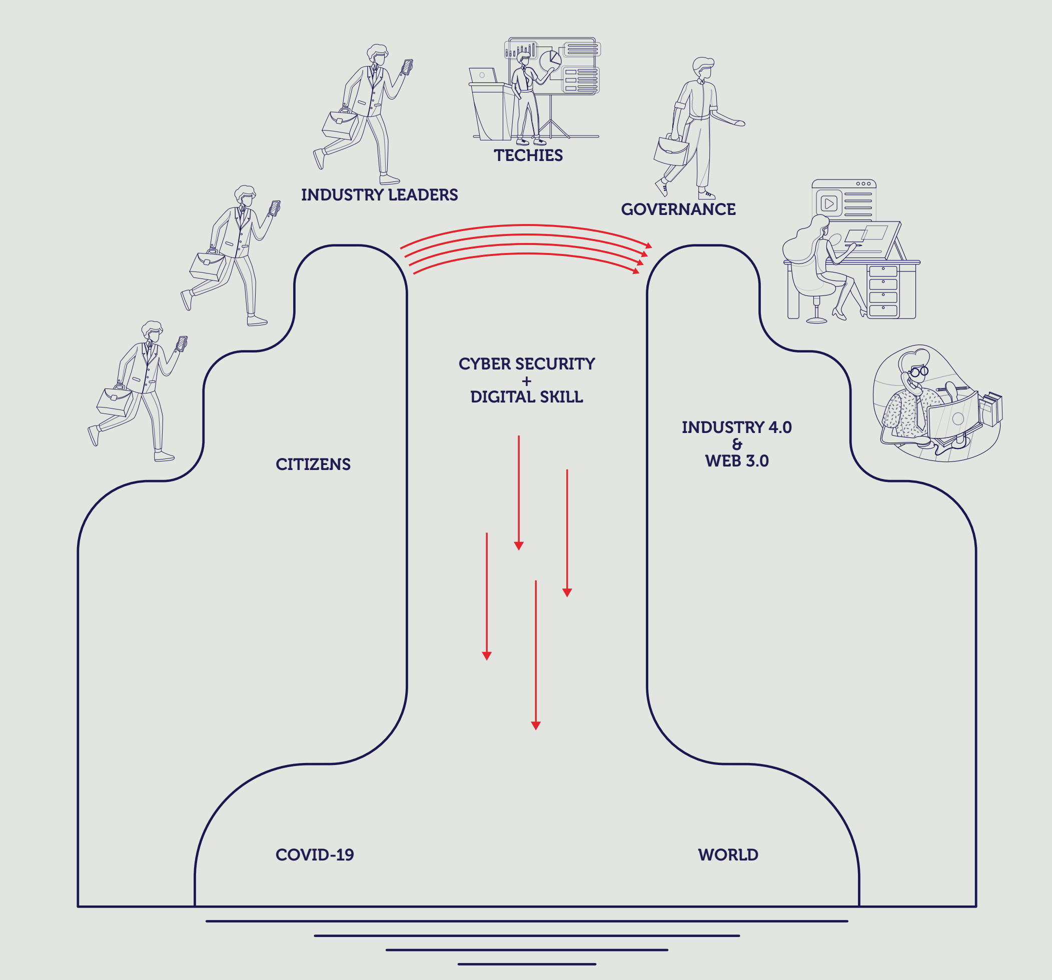


Figure 1: The various roles and skills needed by people in a digitally transformed world.

[35] Bone, J. (2017). Cognitive Hack : The New Battleground in Cyber security ... the Human Mind. (1st ed.). Auerbach Publishers, Incorporated
[36] Sheldon J 'Cyberwar'
[37] Cyber security threat trends: phishing, crypto top the list - Cisco Umbrella
[38] Mattila, M., Yrjölä, M., & Hautamäki, P. (2021). Digital transformation of business-to-business sales: what needs to be unlearned?. Journal of Personal selling & sales ManageMent, 41(2), 113-129.

People as administrators

People need to be positioning themselves as leaders and administrators in cyber space.

An administrator's role includes maintaining and supporting an operating system and associated server hardware, software and databases as well as ensuring optimum system integrity.

This involves planning, developing, installation and troubleshooting. There is also the security, backup and system performance to take into consideration.

An increasingly complex digital infrastructure possesses a variety of unpredictable challenges for urban governance and system administrators. This accounts for the emergence of smart city strategies.[39]

'Smart overarching rules' that permit the space for 'inter-organisational arrangements' and permit polycentric governance that is multi-level, multi-purpose, multi-type and multi-sectoral in scope are required. These rules need to complement the current top-down governance model. They are indications that people who are positioned as national leaders and public administrators across the world are thinking and envisioning a sustainable future incorporating cyber space.[40]

People are an indispensable part of technology development and implementation.

People in organisations

Organisations can be part of the public or private sector with people playing numerous roles as business and industry leaders, managers, specialists and workers.

Networked inter and intra-organisational information systems are mostly large, complex structures that are designed to address the specific needs of organisations that become more complex over time.

Mergers and acquisitions, general growth or obsolescence of legacy systems inevitably change how organisations and their processes operate. Failing to improve the design and engineering of the system, is the reason that enables hackers to succeed.

In today's business world, organisations of all sizes are increasingly exposed to cyber threats, because of unsafe ways of operating and risky online behaviour by staff.[41]

[39] Barns, S., Cosgrave, E., Acuto, M., & Mcneill, D. (2017). Digital Infrastructures and Urban Governance. Urban Policy and Research, 35(1), 20–31.

[40] Shackelford, S. J., & Craig, A. N. (2014). Beyond the new "digital divide": Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. Stanford Journal of International Law, 50(1), 119–184.

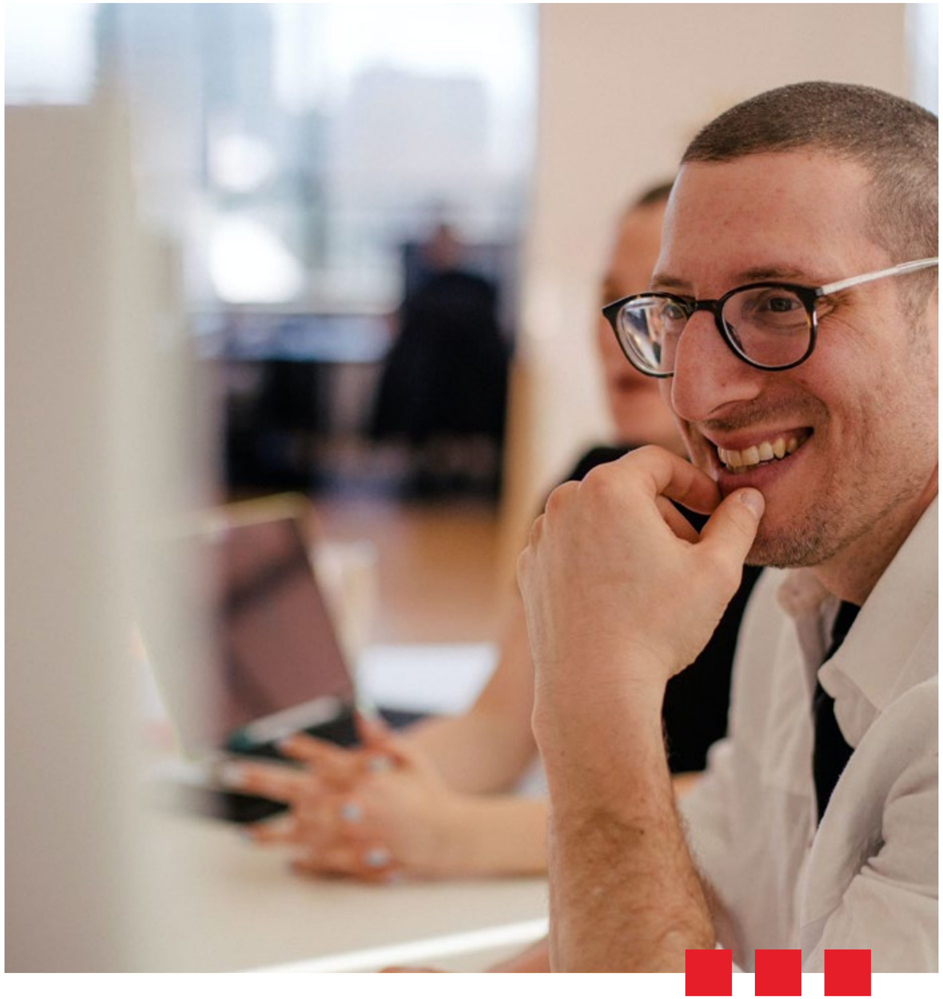
[41] Ibid

People as end-users

Australia has a population of 25.75 million people with an estimated five million living in Melbourne.[42] Based on the 2019 Australian Digital Inclusion Index, Victoria is above the Australian average for internet access (a score of 88.9 for Victoria compared to 87.9 for Australia).[43]

While there is no information at the state level for internet users, the total number of people accessing the internet across Australia as of January 2022 is estimated to be 23.6 million, a 3.4% increase from January 2021.[44] An average of six hours and 13 minutes is spent using the internet per day.

February 2022 saw 19.45 million people purchasing consumer goods via the internet (an increase of 1.2 million from 2021). Suffice to say, Victoria has many end-users engaging with the internet and technology in general.



With this large number of end-users, there is a greater propensity for human error related to cyber and network security such as:

- Sharing passwords
- Oversharing information on social media
- Accessing suspicious websites using unauthorised external media
- Indiscriminate clicking on links
- Reusing the same passwords in multiple places
- Opening an attachment from an untrusted source
- Sending sensitive information via mobile networks
- Not physically securing personal electronic devices
- Not updating software[45]

[42] ABS Regional Population Statistics 2020-21
[43] Thomas, J, Barraket, J, Wilson, CK, Rennie, E, Ewing, S, MacDonald, T, 2019, Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2019, RMIT University and Swinburne University of Technology, Melbourne, for Telstra.
[44] Kemp, S 2022 'Digital 2022: Australia'
[45] Calic, D., Pattinson, M., and Parsons, K. (2016). "Naive and accidental behaviours that compromise information security: what the experts think," in Proceedings of the 10th International Symposium of Human Aspects of Information Security and Assurance, eds N. L. Clarke and S. M. Furnell (Frankfurt: HAISA)

Automation relies on people

The reliance on skilled people underpins a Digital CBD and Industry 4.0. Automation in conjunction with the COVID-19 recession has created a 'double-disruption' scenario for workers.[46]

In a survey published by the World Economic Forum, 43% of businesses indicated that they would reduce their workforce due to technology integration.[47]

Autonomous robots are at the core of Industry 4.0[48] with benefits including increased productivity, less errors, and the performance of high-risk tasks.[49]

However, despite the impact of automation, analysts are still predicting that by 2030, 3.5 million people will be needed to fulfill specific manufacturing vacancies[50] and these people will need to be trained in the required competencies.[51]

PPT Framework

The government, educational institutions and the tech industry have been identified as crucial partners in change.[52]

A popular framework to evaluate information technology management is the **PPT framework**[53] which explores:

1. People – who do the work
2. Processes – that make the work more efficient
3. Technology – which helps people do their tasks

Organisations can achieve organisational efficiency by balancing these three areas and optimising the relationships between people, processes, and technology.[54,55]

[46] World Economic Forum The Future of Jobs Report 2020 (n 12)
[47] Ibid
[48] Kemp (n 44)
[49] Hernandez-de-Menendez, M., Morales-Menendez, R., Escobar, C. A., & McGovern, M. (2020). Competencies for Industry 4.0. International Journal on Interactive Design and Manufacturing, 14(4), 1511–1524.
[50] Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cyber security across the supply chain. International Journal of Production Research, 60(1), 162–183.
[51] Hernandez-de-Menendez (n 49)
[52] Turcu, C., Turcu, C. (2018). Industrial Internet of Things as a challenge for higher education. International Journal of Advanced Computer Science Applications. 9(11), 55–60.
[53] Low, S. P., Gao, S., & Ng, E. W. L. (2021). Future-ready project and facility management graduates in Singapore for industry 4.0: Transforming mindsets and competencies. Engineering, Construction, and Architectural Management, 28(1), 270–290.
[54] Ibid
[55] People, Process, Technology: The PPT Framework, Explained

Defining digital skills

Defining digital skills

Digital skills are fundamental[56,57,58,59,60] and include a "combination of behaviours, expertise, know-how, work habits, character traits, dispositions and critical understandings".[61] Digital skills not only encompass technical skills, but also relate to so-called 'soft skills' such as interpersonal skills and communication skills.[62]

As physical devices and software evolve to meet the new possibilities and demands of the rapidly changing digital world, people's skills will be required to adapt as well.

This is what is often referred to as digital literacy. The term refers to the assortment of thinking strategies that consumers of digital information utilise.[65]

Digital skills are directly influenced by collaboration and indirectly by leadership.[63]

In their study on trends that impact labour markets in preparation for Industry 4.0, Jagannathan et al.[64] found that the key attributes possessed by workers of the future include:

- Digital literacy skills
- Skills for next-generation infrastructure and services
- Skills for technology-infused manufacturing sectors
- Problem-solving skills
- Creativity
- Design-thinking

Information, communication, and technology skills

ICT skills refer to the skills needed to perform various information technology tasks. These skills include talent, knowledge and abilities that relate to the use, development, implementation and management of various forms of technology.[66]

In other words, ICT skills are among the essential competencies that a person needs to possess to fulfill their daily tasks in Industry 4.0.

[56] Jose, R 2021 'Melbourne readies to exit world's longest COVID-19 lockdown'
[57] Australian Curriculum – Information and Communication Technology Capability
[58] Broadband Commission for Sustainable Development Digital Skills for Life and Work Report 2017
[59] What is information technology environment?
[60] United Nations Commission on Science and Technology for Development 2018
[61] Cournoyer, M 2017 'Digital Skills – What are the educational implications?
[62] Futurelearn 2020 'The complete guide to digital skills'

[63] Saputra, N., Nugroho, R., Aisyah, H., & Karneli, O. (2021). Digital skill during COVID-19 effects of digital leadership and digital collaboration. Jurnal Aplikasi Manajemen, 19(2), 272–281.
[64] Jagannathan, S., Ra, S., & Maclean, R. (2019). Dominant recent trends impacting on jobs and labor markets - An Overview. The International Journal of Training Research, 17(sup1), 1–11.
[65] Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. Journal of Educational Multimedia and Hypermedia, 13, 93-106.
[66] Indeed Editorial Team 2021 'Information technology skills in demand today'

Cyber security skills

In practice, cyber security skills are a combination of primary and advanced technical skills that allow an organisation to identify the existing and upcoming cyber risks.

With such skills, a cyber security professional must be able to prepare a plan for current and impending security attacks, risks and threats. This can be done by defining and implementing security frameworks to protect systems and shared information which is often required by law.[67]

In cyber security, some of the fundamental concepts are based on mathematics and other concepts are based on human factors or law.

Conversely, the concept of ICT is not totally related to cyber security.[68] Designing, developing and implementing cyber security can require ICT knowledge and skills.

Many cyber security jobs can be part of the management and board level and this segment of the workforce does not need expertise in ICT.[69]

Developing digital skills through education

In Australia, one in three workers lacks basic digital skills[70] which indicates that a substantial number of workers need reskilling or upskilling.

Reskilling is defined as the process of learning new skills needed to perform an entirely different job while upskilling is defined as adding to an existing skill set within a role.[71]

With rapid digitalisation the workforce, at all levels, will be required to either upskill or reskill in not only advanced technologies but also in cyber security. The workforce will need to be educated, certified and trained to keep up with the rapid developments in technology, science and digital skills through education institutions or certificate programs,[72] through self-learning[73] or free online courses.[74]

Luckily, Victoria is known as the education state of Australia, providing the country with an opportunity to play a leading role in digital skills development and take a leading role in the digitalisation of Melbourne's CBD.

[67] Business.gov.au 'Protect your business from cyber threats' 2021
[68] ACS Cyber security – threats, challenges, opportunities
[69] NIST The Five Functions
[70] New report reveals Australia's major digital skills gap, RMIT 2021
[71] What is reskilling? Why is it so important for today's workforce? 2022
[72] Microsoft Digital skills are in demand. Start building yours today.
[73] Matzat U and Sadowski B 2010 'Does the "Do-it-yourself approach" reduce digital inequality? Evidence of self-learning of digital skills
[74] Future Learn Grow your digital skills with Accenture

Victoria's digital skill responses during COVID-19

The Victorian Government responded to COVID-19 with several programs and initiatives that focused on embracing the acceleration of digital change.

1. The Digital Jobs program facilitated by the Department of Jobs, Precincts and Regions was created to support 5,000 mid-career Victorians to upskill by providing a specific study and work experience framework:

   a. an initial 12 weeks of digital skills training[75] in the areas of cyber security, data analytics, web development, digital marketing or user experience;

   b. followed by a 12-week industry placement in a digitally focused job with a Victorian business such as leading digital companies ANZ, Carsales, Zendesk, Siemens and Salesforce.[76]

2. Universities were supported to provide additional upskilling and training through the Victorian Higher Education State Investment Fund, which invested $350m to support universities with capital works, applied research and research partnerships that had a focus on improving the state's economy, in the wake of COVID-19.[77] Most of the funding allocated was directed towards projects focused on digital transformation, Industry 4.0 and Web3.

3. The Department of Premier and Cabinet released 'A future-ready Victoria – Victorian Government Digital Strategy 2021-2026' in October 2021 which provided a blueprint for how the State of Victoria will invest in digital infrastructure and skills.[78]

4. The Department of Jobs, Precincts and Regions launched the 'Cremorne Digital Hub' in the small inner Melbourne suburb of Cremorne. The Hub is expected to lead a range of activities addressing technology diffusion, digital investment/connectedness, transparency, talent, jobs, and knowledge diffusion.[79]

[75] Ibid
[76] Victoria State Government Digital Jobs
[77] Victoria State Government Support package for universities
[78] Victoria State Government A future - ready Victoria 2021-2026
[79] VPA Cremorne Place Implementation Plan December 2020

The impact of COVID-19

The impact of COVID-19

It has been well-documented that Melbourne was one of the most impacted cities in the world during the COVID-19 pandemic.

The pandemic had a profound impact on the Melbourne way of life and the economy. It also severely affected the supply and demand of digital as well as cyber skills across the city.

Increased digitalisation

One of the first impacts of the global pandemic was the government-mandated working from home restrictions. The shift to working from home advanced the need for robust and high-speed internet connectivity with 45% of Australians working from home and 32% studying online from home.[80]

Digital connectivity through high-speed mobile networks during the pandemic resulted in:

- Businesses and their customers moving to platforms
- Remote working and online collaboration tools
- In-person to online learning
- Adoption of new service delivery models (eg telehealth)[81]

Increased dependency on technology led to the speeding up of advanced technologies. This rapid acceleration resulted in a digital transformation that was spearheaded by the information, communication and technology industry.

The effects of rapid digitalisation during this period were so profound that there were hardly any industries and human lives untouched by it.

[80] ACMA Communications and media in Australia: How we use the internet

[81] Australian Broadband Advisory Council Riding the digital Wave November 2020

[82] ACS Australia's Digital Pulse 2021

[83] ABS More people emigrated from, than immigrated into, Australia in 2020-21

[84] Ibid

[85] State of Australia's Skills 2021: now and into the future

Zero immigration

Skilled migration has always been a significant source for Australia's technology talent pool.[82]

However, the closure of international borders during the pandemic had a negative impact on migration and the technology skills entering the workforce.

There was a decline in overseas migration in every state and territory in Australia, but Victoria was impacted the most with a loss of 56,100 potential migrants.[83] Subsequently, migration in 2021 was almost zero.[84]

The declining population growth, along with the unprecedented rise in advanced and new technologies, manifested in a growing demand for skills in the job market, especially digital and cyber skills.[85]

Unfortunately, the COVID-19-induced drop-in immigration is expected to have significant and lasting effects on the Australian economy.

Increased cyber threats

The rapid digitalisation experienced across the world generated more opportunities for malicious cyber actors to exploit vulnerable targets.[86]

Key cyber security threats include:

- Ransomware
- Disruption to essential services and critical infrastructures
- Exploitation of security vulnerabilities
- Malicious actors targeting
- Supply chains
- Phishing via email[87]

Financial losses due to cyber crime in Australia totalled more than $33b in 2020-2021.[88] Cyber crime mainly occurs through online shopping and banking. Attackers are either low-tech with a high degree of direct offender-victim interaction or high-tech without any interaction.[89]

The most severe incidents are those that affect national security by damaging critical Australian national infrastructure and essential services (eg exfiltrating/deleting highly sensitive data or intellectual property).[90] Most incidents are not as severe but directly affect people and businesses and occur as a result of scamming, phishing or malware/ransomware.

Malware/ransomware is the most destructive and is used 49% of the time to attack large organisations, governments, universities, and supply chains.[91] **These types of cyber crime highlight the need for cyber resilience and digital skills.**

In order to bridge the technology gap, there is a need for the adoption of healthy cyber habits.[92] Such as system vulnerabilities and cyber threats taking into account risks and mitigation as well as countermeasures.[93]

Becoming cyber resilient is considered a main objective for the future, but this can only be achieved when the shortage of cyber professionals is addressed accurately.

[86] ACSC Annual Cyber threat report 2020- 2021 (n 4)
[87] CTPCO Blueprint for critical technologies
[88] ACSC Annual Cyber threat report 2020- 2021 (n 4)
[89] Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016). A typology of cybercriminal networks: from low-tech all- rounders to high-tech specialists. Crime, Law and Social Change, 67(1), 21–37.
[90] CTPCO (n 87)
[91] ACSC Annual Cyber Threat Report 2020-2021 (n 4)
[92] Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. Supply Chain Management, 25(2), 223–240.
[93] Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cyber security for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97–110.

The shortage of digital skills in Australia

Even before the pandemic, Australia was experiencing a shortage of digital skills with the ACS Digital Pulse Report 2019 recommending that the highest policy priority for the digital economy was skills development.[94]

Additionally, the 2019 AustCyber report[95] noted a severe shortage of job-ready cyber security workers which posed a key challenge. The 2016 Australian Information Security Association Study highlighted that around 78% of participants believed that there was a cyber security shortage in the sector.[96]

The ACS Digital Pulse Report 2021 stated that in the first twelve months of the pandemic Australia had increased its technology workforce by 4.3% (33,400 people), which was attributed to the significant increase in demand for digital services.[97] However, this was not the case in Victoria, which experienced a 2% drop in technology workers due to ongoing lockdowns.

Figure 2 provides an insight into the increased demand for digital skills since the twin shocks, with future workforce estimates jumping dramatically in post- COVID-19 industry reporting data.

It also provides insight into the conflicting numbers of digitally skilled workers required across industry organisations and a need for more accurate data for strategic planning purposes.

Pre COVID-19	Post COVID-19
Technology professionals	
The ACS Digital Pulse Report 2019 estimated that there would be an additional **100,000** digital economy jobs by **2024.**[98]	The ACS Digital Pulse Report 2021 estimated that Australia would need to find an additional **300,000** technology workers by 2026.[99] The 2021 Digital Skills Organisation Report estimated that Australia would need to add **60,000** additional digital professionals a year to meet the demand of digitalisation.[100]
Cyber security professionals	
The 2019 ACS Digital Pulse Report estimated a need for around **17,000** additional cyber security workers for technical as well as non-technical positions by **2026**.[101]	2021 ISC2 Workforce Study estimated around **25,000** cyber security professionals just to close the current gap in the marketplace.[102]

Figure 2: Increased demand of digital skilled workers due to the twin shocks

[94] ACS Australia's Digital Pulse 2019
[95] AustCyber Australia's Cyber Security Sector Competitiveness Plan 2019 Update
[96] ASIA The Australian Cyber Security Skills Shortage Study 2016
[97] ACS Australia's Digital Pulse 2021 (n 82)
[98] ACS Australia's Digital Pulse 2019 (n 94)
[99] Ibid
[100] Towards a new model for the development of digital skills 2021
[101] AustCyber Australia's Cyber Security Sector Competitiveness Plan 2019 Update (n 95)
[102] ISC Cyber security Workforce Study 2021

Melbourne Digital Skills Survey 2022

Effect of COVID-19 on Melbourne's digital professionals

To provide further insight into the current skills shortages in the Victorian labour market, we surveyed 136 digital professionals including ICT & cyber professionals, who worked in greater Melbourne.

Our respondents worked directly in information technology and cyber security (29%) with an additional 6% from telecommunication, 12% from Federal and State Governments and 18% from education. Approximately 80% were employed full-time.

How did the pandemic affect the work-life of the digital professional?

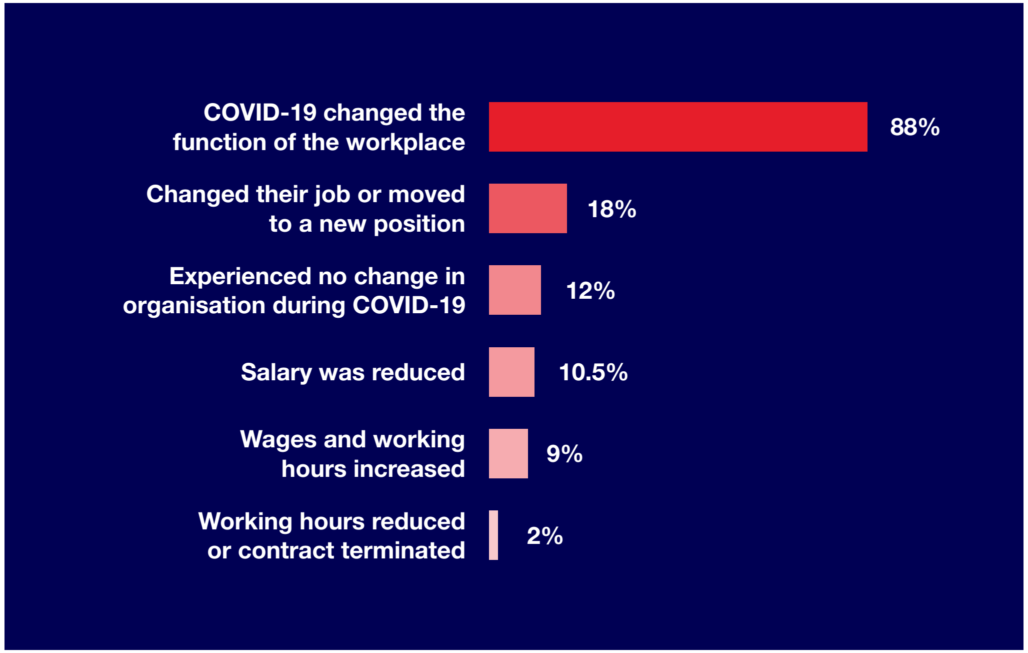
The pandemic had a profound effect on digital professionals, with Melbourne experiencing the longest lockdown globally; 262 days [in total]. Which is almost nine months.[103] Their work, occupation and their organisations were impacted in some way.

During this time, 18% of respondents changed their job, or moved to a new position, some have alluded to this collective action as the "great resignation"[104], and 6% changed their roles within the same organisation. Under 2% of workers had their paid working hours reduced or had their contract terminated. However, 10.5% of employees indicated that their salaries had been reduced. The good news is that 43% of respondents saw no change in their working status, while 9% of respondents said that their wages and working hours increased. Interestingly, 88% of respondents indicated that COVID-19 changed the function of their organisation in different ways, whilst 12% did not experience any change in the last two years.

When these results are set against the backdrop of education, nearly 51% of respondents had completed a postgraduate degree and 37% had an undergraduate degree. This indicates that the digital and cyber sector attract a highly-educated workforce who have the fundamental skills to learn, impart, and, grow with the needs and demands of the industry.

Organisations of less than 1,000 workers employed 58% of respondents and nearly 15% of the respondents worked in organisations with more than 10,000 employees.

The findings above indicate that highly-educated and skilful professionals are resilient in the face of setbacks (such as pandemics) and adapt to the ways their organisation might change over time.



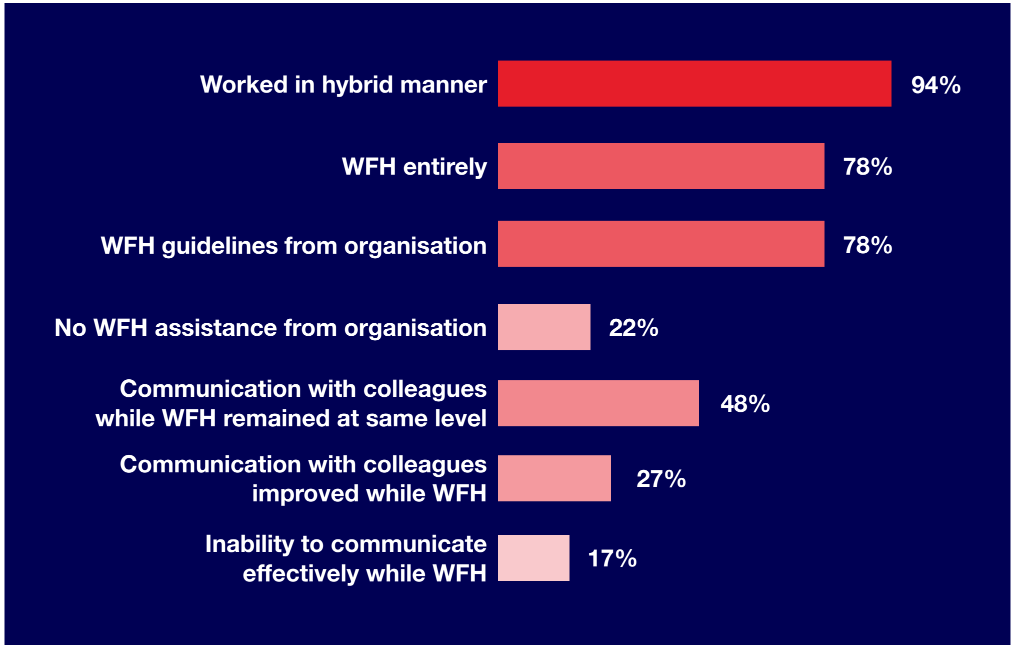
[103] Jose, R (n 56)

[104] Sharples, S 2022 'The great resignation hits Australia as 1 million people quit their jobs'

How the working arrangements of digital professionals were affected

The COVID-19 pandemic forced 94% of respondents to work in a hybrid manner with 45% working entirely from home (WFH) and 78% conveying that their organisation developed specific WFH guides and policies for their employees in response to COVID-19. However, 22% of respondents were dissatisfied with the transition to WFH as they did not receive help.

Post-pandemic, nearly 12.5% preferred continuing with the WFH policy, 39% indicated that they would prefer to WFH for most of the time and nearly 11% of respondents indicated that their organisation would like them to return to their usual workplace.



With an increase in people working from home, the greater the attack surface and the greater the threat of cyber security attacks.

Effective communication has become a key challenge as most employees are working from home. 48% of respondents indicated that the quality of communication with co-workers in the context of remote working environments stayed at the same level and 27% indicated that communication had improved. Worth noting is the 17% of respondents who experienced an inability to communicate effectively amongst family indicating that it that it will be necessary to delve deeper into this cross-section in the future to comprehend how much this lack of communication will affect work.

The majority of respondents (66%), indicated that the two most profound challenges in keeping the workforce secure were the lack of security awareness among remote workforces and keeping up with the latest cyber security threats. In comparison, 21% believed the rapid deployment of new collaboration tools was a critical problem in keeping the workplace secure.

Digital technologies and digital skills

Significant investment in new technologies, but is it enough?

Despite cyber security being a big focus over recent years, 2020 and 2021 still brought about several high-profile cyber attacks.

With the pandemic forcing many to work from home, organisations had to rapidly invest in appropriate technologies to help sustain productivity. The survey highlighted that approximately 70% of respondents invested in additional technology. Unsurprisingly, a quarter of respondents (25%) invested more into their cyber security infrastructure.

Despite cyber security being a big focus over recent years, 2020 and 2021 still brought about several high-profile cyber attacks, both nationally and internationally.

Statistics presented by the Australian Cyber Security Centre (ACSC) indicated that during the 2020-2021 financial year there were over 67,500 cyber crimes reported – an increase of nearly 13% from the previous financial year.[105] This equates to around one cyber attack occurring every eight minutes. Businesses, individuals and other entities incurred more than $33b in total losses from cyber crime throughout the same financial period.[106]

The ACSC responded to about 1,630 cyber security incidents in 2020-21 (or an average of 31 cyber security incidents a week). Approximately one-quarter of reported cyber security incidents affected critical infrastructure organisations including essential services such as education, health, communications, electricity, water, and transport.[107]

While the investment in cyber security is appropriate, it is smaller than anticipated given the importance of developing cyber security resilience to meet the challenges being presented.

Over the last two years, other significant investments included computers and laptops (18%) followed by web cameras (8%) and smartphones (7%) with approximately 8% of respondents investing in IoT technologies.

However, when identifying technologies that organisations plan to implement in the next two years, approximately 21% of respondents indicated they would be investing in cyber security as well as exploring technologies including AI (14%), the IoT (11%), ML (10%) and computers or laptops (10%).

This indicates a shift from previous years to more of a focus on cyber security and Industry 4.0 technologies.

Top 5 digital technologies that organsiations plan to invest in:

1. **Cyber security**
2. **Artificial Intelligence**
3. **Internet of Things**
4. **Machine learning**
5. **Computers/laptops**

[105] ACSC Annual Cyber Threat Report 2021 (n 4)
[106] Hurst, D 2021 ‘Significant threat: cyber attacks increasingly targeting Australia’s critical infrastructure’
[107] ACSC Annual Cyber Threat Report 2021 (n 4)

How are organisations placed in terms of the digital skills of their employees?

Given the investment and exploration of new technologies, organisations need to be prepared in terms of the digital skills of its employees. Digital transformation within organisations is less about technology and more about people.[108]

The World Economic Forum (2021) indicated the emphasis on human capital as part of digital transformation, explicitly stating that "malicious actors are increasingly targeting the weakest link in tech systems: the human beings who interact with them."[109]

Approximately 55% of respondents indicated that their workforce had the right digital skills, meaning that the remaining 45% felt the need to invest in upskilling the digital skills of their employees.

Most of the respondents (65%) were looking for advanced digital skills, while 35% of respondents were looking for entry-level digital skills.

Cyber security was the top skill that organisations were looking for, followed by entry-level computer literacy.

Advanced digital skills of data science, digital design, digital visualisation, and user experience designer were also highly rated by respondents.

Top 5 advanced digital skills required:

1. **Cyber security**
2. **Data science**
3. **Digital design**
4. **Data visualisation**
5. **UX design**

Cyber security was the top skill that organisations were looking for, followed by entry-level computer literacy.

[108] Frankiewicz, B., & Chamorro-Premuzic, T. (2020). Digital transformation is about talent, not technology. Harvard Business Review, 6(3).
[109] De Moura, G and Kostopoulos, L 2021 'Here's why closing the cyber security skills gap is critical to digitalization'

Cyber security skills

Number of cyber security professionals growing slowly

Approximately three-quarters of respondents indicated that their role included a cyber security aspect. Australia currently has 805,525 employees working in technology and 134,690 cyber security professionals.[110,111]

Relatively speaking, our survey reflects these numbers and is heavily influenced by the particular views of those working in these industries.

Unsurprisingly, over half of our participants considered cyber security to be the most vital in terms of digital skills. The majority of participants echo this sentiment and indicated that they are genuinely concerned about cyber security threats and believe that they need to upskill to meet the demands of the industry.

These results highlight the dire need for the development of cyber security courses on all levels if we want to ensure Melbourne is protected against cyber attacks.

Although over 60% of respondents indicated that there has been an increase in the number of cyber security staff compared to three years ago, only a quarter of respondents believe that they currently have enough cyber security professionals working in their organisation.

Only a quarter of respondents believed that their organisation currently had an adequate number of cyber security professionals.

Of the 70% of respondents who indicated that they have noted a skills shortage in their workplace, 43% believe there is a significant shortage and 27% believe there is a slight shortage.

Much effort has gone into growing the cyber security workforce in Australia – though it has not proven to be enough yet. At this very moment, we cannot safeguard our businesses, people and the future of our city against looming cyber security threats.

[110] ACS Australia's Digital Pulse 2021(n 82)

[111] ISC Cyber security Workforce Study 2021 (n 102)

COVID-19 compounded cyber security skill shortages within organisations.

Over 40% of respondents indicated that COVID-19 had a negative impact on their organisation's ability to employ staff who possess appropriate cyber security skills.

This is especially problematic when measured alongside the fact that 54% of respondents felt that their organisation's response to the pandemic had left them more exposed to security threats.

60%

Increase in cyber security staff compared to three years ago

25%

Has adequate cyber security staff

70%

Noted a shortage of skills in workplace

40%

COVID-19 had negative impact on organisation

54%

COVID-19 left organisation more exposed to security threats

The areas in which cyber security professionals feel the need to upskill

Nearly all of our cyber security respondents indicated that they would like to improve their skills and enhance their knowledge over the next two years: 26% said they would like to do this through hands-on training, 22% indicated that they required to deepen their knowledge to upskill, and 19% would like to improve their leadership skills:

- **Technical skills (hands-on training)**
- **Broader knowledge base**
- **Management and leadership skills**
- **Soft skills**
- **Board and Director skills**

Role of individuals and industry in training and qualifications

How have digital professionals invested in training and qualification?

According to 79% of respondents, cyber security certification is the most beneficial qualification to their careers. Having a cyber security certification within the first twelve months of employment is important to 24% of respondents and 21% are planning on being certified before getting their first role in the cyber security industry.

There is a window of opportunity to attract 21% of respondents who are still not sure when the best time is to upgrade their knowledge.

In terms of how respondents would like to upgrade their knowledge, 61% indicated that on-the-job training was the most favoured. Approximately 22% indicated that higher education is their preferred method and only 4% of respondents thought an industry certificate in IT would suffice with 3% of respondents interested in micro-credentials, diplomas and/or certificates in IT.

Just over 56% of respondents believed that they needed to upskill within the next three to six months, while another 32% think that they need to do so in the next six to twelve months.

Finally, approximately 21% of respondents wanted to obtain a border knowledge base.

These skills can include knowledge of contemporary fields such as information and communication technology, algorithms, automation, software development and security, data analysis, general systems theory and sustainable development theory.[113]

Such skills are varied, ranging from managing complex manufacturing systems to skills that incorporate more creative aspects, such as strategic/design thinking, creativity, strategic thinking and coordination skills.[114]

Management and leadership skills

Management and leadership skills are important attributes for the growth and sustainability of the digital profession and can be a combination of lifelong learning and continuous training.

Interestingly, only 24% of respondents indicated they needed to focus on developing their management and leadership skills within the next two years.

Existing managers, leaders and executives need to play a multifaceted role of being creative innovators, change agents, strategic partners and people enablers in order to take advantage of the opportunities of Industry 4.0 and mitigate associated challenges. They also need to mentor their team to aspire to be leaders of the future through lifelong learning and training.

Skills in leadership include the strategic vision of knowledge, self-organisation, giving and receiving feedback, pro-activity, creativity, problem-solving, interdisciplinarity, teamwork, collaborative work, initiative, communication, innovation, adaptability, flexibility and self-management.[112]

[112] Kipper, L. M., Iepsen, S., Dal Forno, A. J., Frozza, R., Furstenau, L., Agnes, J., & Cossul, D. (2021). Scientific mapping to identify competencies required by industry 4.0. Technology in Society, 64, 101454–.

[113] Ibid

[114] Hecklau, F., Galeitzke, M., Flachs, S., Kohl, H.(2016).: Holistic Approach for human resource management in Industry 4.0. Procedia CIRP 54, 1–6.

What role does industry play?

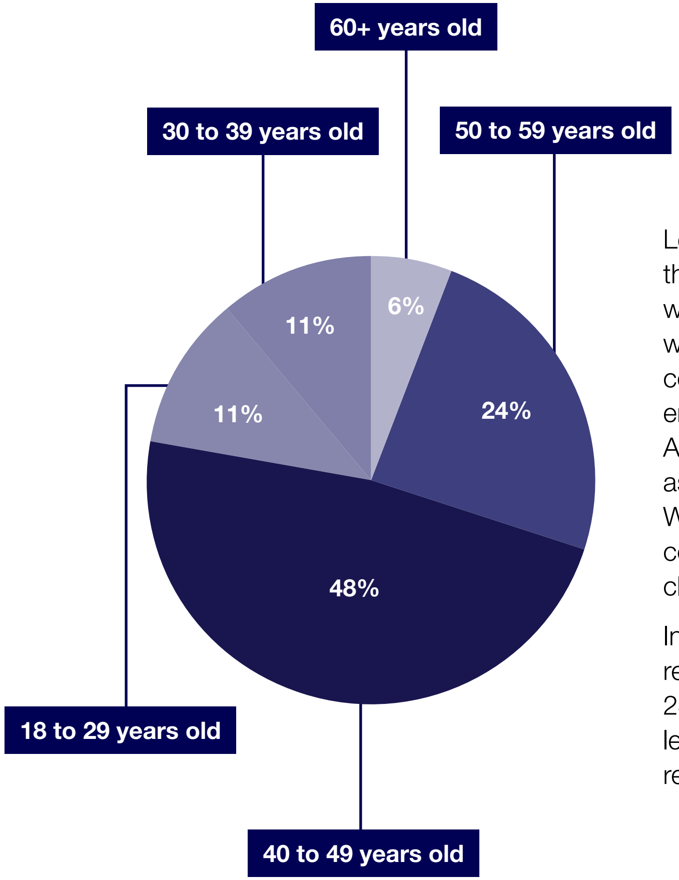
Investment in cyber security training and education within the next 12 months is one of the pathways to develop and cultivate the talent pool. Three-quarters of the current talent profile have an IT qualification and just over half agree that their organisation regularly supports them to upskill their knowledge. Delving further into the issue of support on the job, 53% of respondents confirm that their organisation invests in such training and 38% believe that there is no change. This indicates that the industry is set for a highly skilled talent pool.

The industry needs to note that there are two key factors that will determine the composition of the talent pool.

1. The first concern is the aging workforce with nearly a quarter of respondents aged 50 years or older. This indicates a retiring segment within the next 20 years[115] and with it, years of intellectual property.

2. The second concern is the lack of diversity in the talent pool. Gender diversity, women's inclusion, and male dominance in the technology industry have been discussed for quite some time.

More diversity and inclusion could help to close this gap.



Less than 15% of workers in the cyber security industry are women, making it the industry with the biggest gender gap.[116] compared to 44% of women employed as ICT professionals in Australia.[117] Luckily, not-for-profit associations like the Australian Women in Security Network[118] continue to advocate to close this gap.

In this study, 72% of respondents were male and 23% were female which is less than one third representation of women.

[115] Depart of Social Services Age Pension
[116] Bhosale, P, 2022 'How to close the cyber security gender gap'
[117] Statista 'Share of women in ICT occupations in Australia as of 2020'
[118] Australian Women in Security Network

Recommendations

Based on the research findings,

we propose the following recommendations to address the of ICT and cyber security skills gap.

Recommendations

Recommendation 1: Establish a Victorian Digital Skills Academy

It is evident that the current digital skills gaps will not be closed and that an alternative course of action is urgently needed.

For Melbourne to maintain its momentum towards becoming a leading Digital CBD, the Victorian Government should consider investing in a **Digital Skills Academy**.

There is a significant investment from government, industry, and the higher education sector in digital skills. However, this disjunctive approach is not accurately tackling the problem of an under skilled workforce in Victoria.

A government intervention to bring all stakeholders together, in a combined collaborative approach will have a greater impact in developing the workforce Melbourne requires for a secure and resilient future.

The Digital Skills Academy would be responsible for increasing the number of digital professionals.

Recommendation 2: Establish an Australian Cyber Security Accreditation Body and an Australian Cyber Security Body of Knowledge

Historically, Australia's professional organisations have attempted to accredit Australian cyber security courses, albeit with limited success. Therefore, Australia needs to establish a:

- **Cyber security accredited industry body**, with representatives from all stakeholders such as industry, government and higher education to develop a national cyber security accreditation process.
- **Cyber Security Body of Knowledge (CSBoK)**, would fully prescribe what should be taught within Australian cyber security courses from technology, organisational perspective.

  The CSBoK would need to be developed in partnership with industry, professional bodies, and higher education institutions to ensure that Australian cyber security courses reflect the current thinking and requirements of industry.

Address the ICT and cyber security skills gap so that Melbourne can move towards a Digital CBD.

Recommendation 3: Create a comprehensive ICT and Cyber Security Diversity Action Plan for Victoria

To improve diversity, the Victorian Government needs to lead an initiative that brings higher education, industry and government sectors together to encourage the participation of women and First Nations people into the industry.

Therefore, the creation of an **ICT and Cyber Security Diversity Action Plan for Victoria** is recommended.

Actions to be implemented into the plan include dedicated scholarships, specific cohort programs, mentoring programs and diversity targets and quotas.

A focused diverse representation will not only create new channels in the talent pipeline but also add richness to the experiences and backgrounds of these representatives.

The infusion of a diverse talent pool will create strong mentorships and the extrapolation of knowledge and experiences culminating in a sustainable and thriving workforce.

All Melbourne CBD businesses/training providers/partners should be supported and incentivised to design their own Gender Action Plans.

Recommendation 4: Increase skilled migration to aid Victoria's recovery

Skilled migration has been a significant contributor to the Australian digital workforce.

However, migration reaching almost net-zero during COVID-19 has significantly contributed to broadening the digital skills gap.

The Victorian Government needs to:

- Lobby the Federal Government to increase the total number of skilled migrants into Australia; and
- Develop an innovative migration program promoting the benefits of Melbourne to digital professionals globally. Tactics could include activities such as advertising Victorian international job vacancies, a concierge service to assist new migrants settling into Melbourne, and marketing initiatives at key digital events around the globe.

Recommendation 5: Invest in innovative school programs highlighting the skills required in a digital economy

More needs to be done to increase and diversify the number of school age students that aspire to join the ranks of the digital economy in line with the increasing demand for digital skills.

To position Melbourne as a Digital CBD, Victoria will need to encourage a diverse range of students to enter digital pathways much earlier in their education.

There are many school-based programs, however these are administered in an ad-hoc fashion and are often extracurricular rather than core courses included into the curriculum. It is recommended that students are exposed earlier in their learning journey to the digital world.

Recommendation 6: Create a program to increase the awareness of digital technologies and the need to upskill digital skills within the Melbourne CBD

As identified in this report, to realise the true benefits of a Digital CBD we need the people of Melbourne to be users and adopters of technology.

There is a risk that our most vulnerable people will get left behind and that a divide occurs between those that are digitally savvy and those that are not.

Digital skilling does not just refer to the technical ICT and cyber security skills required to underpin a Digital CBD but also ensures a basic level of digital skills for everyone so that they can engage within the digital community.

This may mean that community centres need to be established that assist people in their digital upskilling. Outreach programs may need to be established to ensure minority groups, the elderly and new migrants have the required level of digital skills to engage with the Digital CBD.

RMIT
UNIVERSITY