Victoria's Cyber Strategy 2021

Mission Delivery Plans
2021-2022

VICTORIA
State
Government

Authorised and published by the Victorian Government Melbourne April 2021

This document is also available in Word and PDF format at www.dpc.vic.gov.au

ISBN 978-1-925789-62-1 **(pdf/online/MS word)**

Acknowledgment of Country

The Victorian Government acknowledges Aboriginal and Torres Strait Islander people as the Traditional Custodians of the land.

The Victorian Government also acknowledges and pays respect to the Elders, past and present and is committed to working with Aboriginal and Torres Strait Islander communities to achieve a shared vision of safer and more resilient communities.

Table of contents

Flinders Street

Victoria's Cyber Strategy 2021

1

Government, industry and individuals face constant threat from cyber criminals, organised crime groups, online vandals, trusted insiders, advanced persistent threat groups and foreign governments.

Victorian Government IT networks face constant threat of cyber-attack. Private companies face similar challenges, with malicious cyber attackers constantly threatening to disrupt vital systems and services.

Australians report a new cyber-attack to the Australian Cyber Security Centre every 10 minutes. One-in-four of these reports involves Victorians who have fallen victim to malicious cyber activity, such as online scams and fraud.

The financial, emotional and service delivery impacts of malicious cyber activity are significant. Industry estimates suggest the cost of cybercrime to the Australian economy is $29 billion annually.

Responding to this challenge requires strong collaboration across government, industry and the community. We all have a role to play in creating a cyber safe Victoria.

The Victorian Government must continually enhance the protection of its IT networks to support the safe and reliable delivery of services. We must also support industry and community groups to reduce their cyber risk. Success in these areas relies also on an ability to build a vibrant cyber economy that provides access to local skills, knowledge and tools.

Victoria's Cyber Strategy 2021 outlines the Victorian Government's priorities and approach for improving Victoria's cyber resilience.

The strategy will be delivered through three core missions:

1. The safe and reliable delivery of government services
2. A cyber safe place to work, live and learn
3. A vibrant cyber economy.

The Mission Delivery Plans detail the actions that will commence in 2021-22 in support of these missions.

Mission Delivery

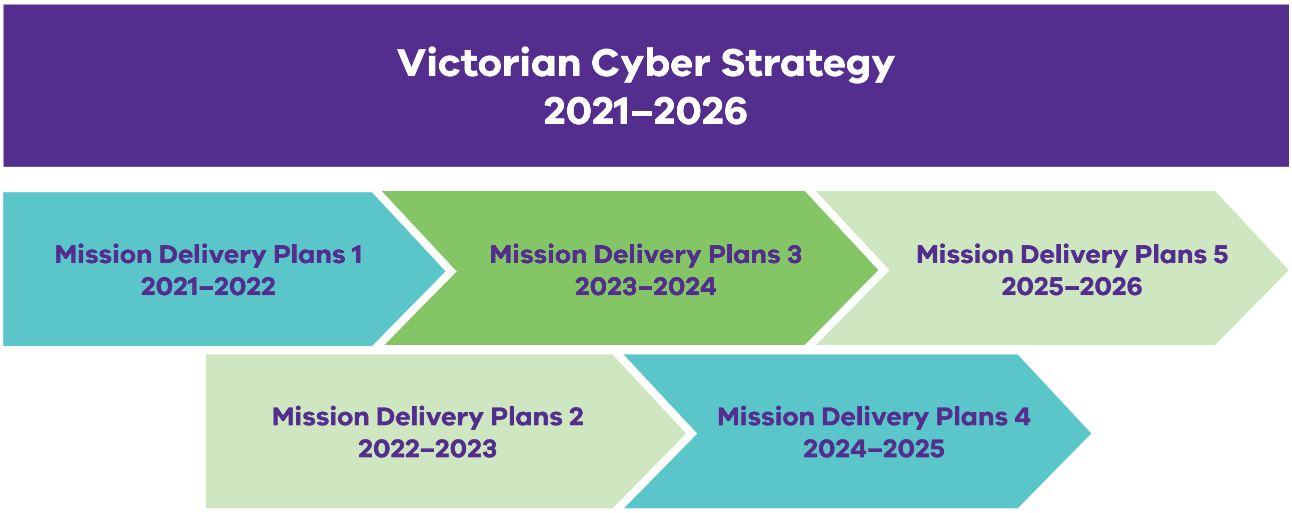
2

The actions associated with Victoria's Cyber Strategy 2021 are detailed in the Mission Delivery Plans. The plans were developed in consultation with relevant stakeholders across government and industry.

The development of the Mission Delivery Plans acknowledges the rapidly changing digital environment and the evolving cyber risks faced by government, industry and the community.

The Victorian Government Chief Information Security Officer will publish an annual statement on the progress of actions identified in the Mission Delivery Plans.

Victoria's Cyber Strategy 2021 – Relationship with the Mission Delivery Plans



Victorian Cyber Strategy 2021–2026

Mission Delivery Plans 1 2021–2022

Mission Delivery Plans 3 2023–2024

Mission Delivery Plans 5 2025–2026

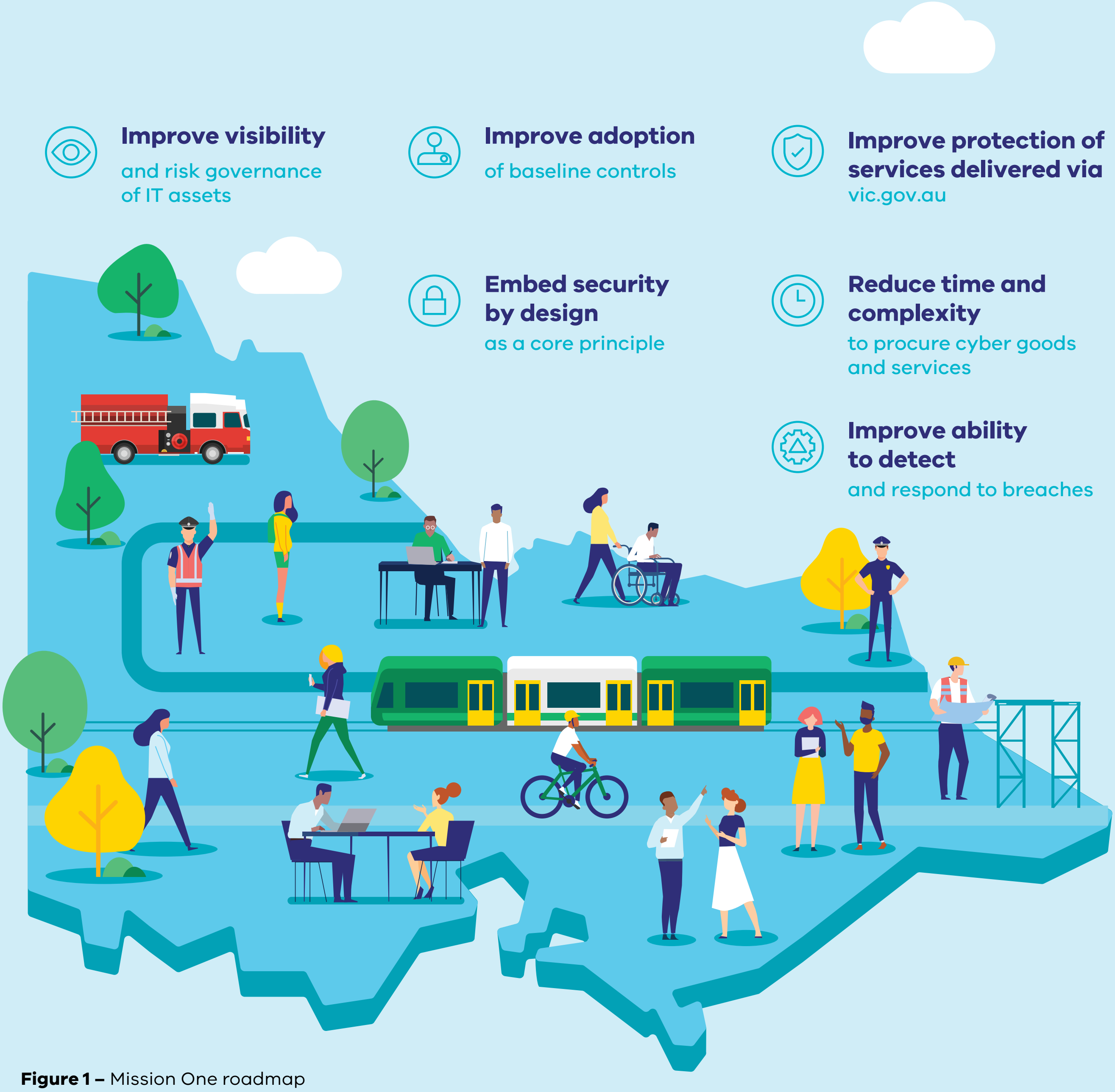
Mission Delivery Plans 2 2022–2023

Mission Delivery Plans 4 2024–2025

3

Mission One

The safe and reliable delivery of government services



Improve visibility and risk governance of IT assets

Improve adoption of baseline controls

Improve protection of services delivered via vic.gov.au

Embed security by design as a core principle

Reduce time and complexity to procure cyber goods and services

Improve ability to detect and respond to breaches

Figure 1 – Mission One roadmap

Introduction

Victorian Government IT networks face constant threat of cyber-attack.

These incidents include online scams and fraud, malware and denial-of-service attacks, and the defacement of government websites. They threaten the safe and reliable delivery of government services and the confidentiality of sensitive and personal information.

Mission One aims to strengthen the defences of Victorian Government networks and services equal to the current and emerging threats. This mission will protect the confidentiality and integrity of sensitive information and support the reliable delivery of IT-dependent government services to the Victorian community.

Mission One priorities

Key priorities for Mission One include:

The privacy of sensitive information held by the Victorian Government is protected

The Victorian Government creates, collects and holds a significant amount of sensitive and personal information. From people's medical records, to sensitive police data, this information could cause harm to individuals, the community, the economy or the government if made available to the wrong people. This information must be protected to reduce the potential for harm.

Services delivered either online or in the physical world are resilient to cyber-attacks and can be quickly recovered when interrupted

Online services are often a cost effective and convenient way for Victorians to interact with government. From obtaining a property title to renewing a license, online service delivery provides quick, easy and convenient access to government services. Further, many services delivered in the physical world such as trains, hospitals and water systems are reliant on IT systems. The Victorian Government has a responsibility to ensure the IT systems supporting these services are resilient to cyber-attacks.

Digital communications channels are trustworthy and free from manipulation

The Victorian Government communicates with businesses and individuals via multiple digital channels such as email, social media, online forums and websites. We have a responsibility to maintain public confidence in the authenticity of these communications by reducing the potential for manipulation.

Scope

Mission One incorporates the entirety of the Victorian Public Sector as defined by the Victorian Public Sector Commission. The sector comprises 1,817 agencies including 47 public service departments and offices, 1,544 school councils and 226 other public entities. In 2020 the Victorian Public Sector employed around 322,050 people, representing nine per cent of Victoria’s workforce (correct at time of publishing).

Target state

Analysis of local and international data shows that while cyber-attacks continue to increase, the most commonly successful cyber-attacks can be prevented by using proven and effective controls. Government will ensure that IT systems it uses implement a range of baseline information security controls. Critical services will be required to meet a higher minimum standard, which are fit-for-purpose and highly resistant to cyber-attacks.

In line with industry standards, the minimum expectation for government IT systems are:

Identify

We know what IT systems support government services, and we know where data supporting these services resides both within and outside our networks.

All information types and IT systems have been assessed for the harm that would occur if a breach of confidentiality, integrity or availability was to occur.

The monitoring and identification of IT systems occurs in near real time.

We understand our threat environment – our cyber-attackers, their motives and their methods. We centrally develop and share intelligence that reduces cyber risk for the public sector.

Protect

All systems have implemented known effective baseline controls to protect against common attacks, including the Essential Eight.[1] Critical services are highly resistant to cyber-attacks.

Detect

All systems can detect common and unsophisticated attacks. Critical systems can detect sophisticated attacks.

Respond

All government organisations document and test processes for responding to cyber security incidents. These processes are aligned with the State Emergency Management Plan (Cyber Security Sub-Plan) and the Victorian Government Cyber Incident Management Plan. These processes are exercised annually (at a minimum) and updated regularly to support a continuous improvement cycle.

Recover

All government and critical services can be recovered within a timeframe determined by the entity executive. This recovery process is regularly tested.

Actions

Improve visibility and risk governance of IT assets

1.1 Develop an IT asset management guideline in line with Asset Management Accountability Framework (AMAF) and Victorian Protective Data Security Framework (VPDSF) requirements.

1.2 Develop and make available to Whole of Victorian Government (WOVG) training material on IT asset management guideline for both IT staff, line managers and executives.

1.3 Deploy with Victorian Managed Insurance Authority (VMIA) an Essential Eight status monitoring program.

1.4 Work with the National Cyber Security Committee to standardise government third party supplier security frameworks across Australian jurisdictions.

[1] The Essential Eight is a series of baseline mitigation strategies taken from the ACSC's ***Strategies to Mitigate Cyber Security Incidents*** recommended for organisations. Implementing these strategies as a minimum makes it much harder for adversaries to compromise systems. You can learn more about the Essential Eight at https://www.cyber.gov.au/acsc/view-all-content/essential-eight.

Improve adoption of baseline controls

1.5 Issue guidance on the successful implementation of the Essential Eight.

1.6 Issue Victorian Government recommended security configuration for Office365.

1.7 Issue guidelines for accessing classified information and security clearances for staff within Victorian Government entities.

Improve protection of services delivered via the vic.gov.au domain

1.8 Commence decommissioning unused services currently active on vic.gov.au domains.

1.9 Commence Domain-based Message Authentication, Reporting and Conformance (DMARC) implementation across all email services using the vic.gov.au domain.

Embed security by design as a core foundation principle

1.10 Establish a WOVG Third Party Risk program, embedding security by design as a foundational principle.

1.11 Establish central security architecture capability.

Reduce time and complexity to procure cyber goods and services

1.12 Establish a simple procurement process for Essential Eight related goods and services.

1.13 Set up a deed of standing offer with one or more preferred anti-malware service providers.

1.14 Set up a deed of standing offer with one or more suppliers of IT asset discovery and monitoring tools.

Improve ability to detect and respond to breaches

1.15 Issue log collection and retention guidelines.

1.16 Set up a deed of standing offer with Security Operations Centres (SOC) for critical services.

1.17 Establish a WOVG proactive threat hunting capability to detect new and emerging cyber risks.

Improve resilience of critical services

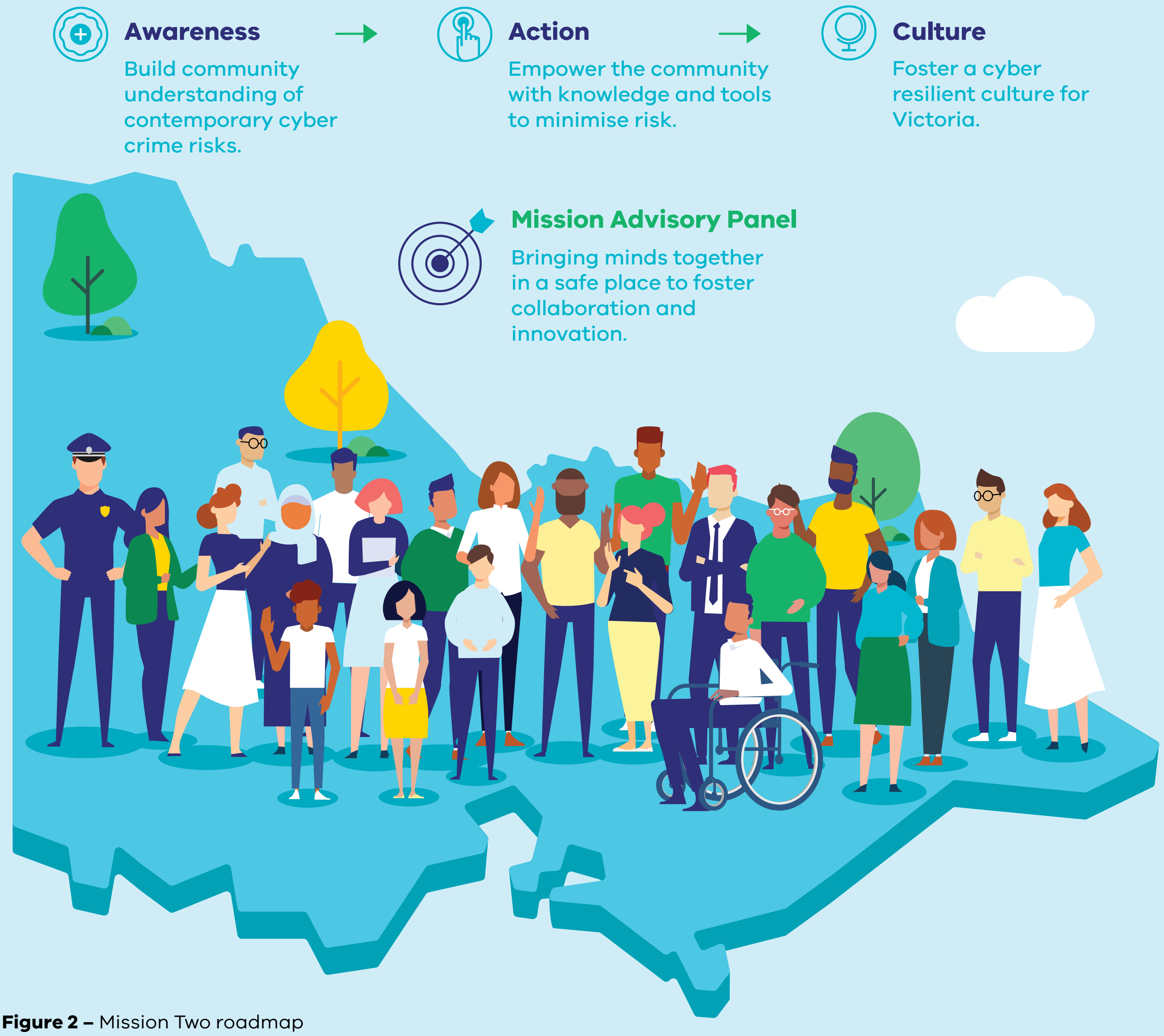
1.18 Undertake a cyber education program for government executives in critical service operations.

1.19 Work with critical service operators, other states and the Australian Government on issuing consistent cyber regulation and standards for critical services.

Mission Two

A cyber safe place to work, live and learn

4



Awareness → Build community understanding of contemporary cyber crime risks.

Action → Empower the community with knowledge and tools to minimise risk.

Culture Foster a cyber resilient culture for Victoria.

Mission Advisory Panel Bringing minds together in a safe place to foster collaboration and innovation.

Figure 2 – Mission Two roadmap

Introduction

All Victorians who use digital systems and services will experience some level of cyber risk. Data from the Australian Cyber Security Centre shows that too often Victorians are falling victim to these cyber risks, with a new cybercrime reported in Victoria every 40 minutes.

Mission Two aims to support individuals, households, businesses and community groups to connect, engage and work safely online. We will align community engagement, education, legislation, policing and emergency management arrangements to foster a cyber resilient culture for Victoria.

Mission Two priorities

Key priorities for Mission Two include:

Victorians receive practical advice about how to reduce cyber risks

Cybercrime is increasing in scale and sophistication. One in four cybercrime reports to the Australian Cyber Security Centre affects Victoria. Understanding of cybercrime varies across government, businesses and the community. The opportunity exists to provide Victorians with clear and practical advice about cyber risks, including cybercrime, to reduce the likelihood and extent of harm.

Police are supported to prevent, detect, disrupt and prosecute cybercrime and other online offending (including technology-enabled crime)[2]

Cybercrime is a global issue with local impacts. The growing role of technology in crime presents a pressing and urgent challenge for law enforcement agencies around the world. Technology is used by criminals to support, enable, hide and increase the efficiency of their criminal enterprises, including serious and organised crime, online sexual offending and family violence. Police need the skills, tools and powers to combat this growing challenge, now and into the future.

Critical infrastructure owners and operators, and essential service providers, are supported to improve their cyber resilience

Technology is integral to the operation of critical infrastructure and essential services. Critical infrastructure is an attractive target for malicious cyber activity. Cyber-attacks against critical infrastructure and essential services can have significant consequences for the community and our environment. Critical infrastructure and essential service providers should be empowered and supported to combat cyber risks.

Target state

The Victorian Government will create a cyber safe place for Victorians to work and live through appropriate legislation, policing and emergency management arrangements.

We want individuals, households, businesses and community groups to be resilient to cyber risks, allowing them to connect, engage and transact safely online.

Victoria's critical infrastructure and essential service providers should be supported to enhance their cyber resilience and mitigate service disruptions.

Actions

Improve understanding of cyber risks, issues and response opportunities

2.1 Establish an Expert Advisory Panel to provide insight on current and future cybercrime risks, issues and response opportunities, and identify future risk mitigation strategies.

[2] Cybercrime is defined as crime directed at computers or other IT systems/assets; and technology-enabled crime.

2.2 The Expert Advisory Panel should report to government on opportunities to:

a. Enhance cybercrime messaging and education programs for government, industry and the community

b. Reduce the community impact and harm associated with cybercrime

c. Consider legislative reform opportunities to help police combat cybercrime.

Improve cyber support for Victoria's critical infrastructure and essential services

2.3 Continue to build on engagement with the Victorian Government Critical Infrastructure Sector Resilience Networks and the Critical Infrastructure Resilience Sector Forum to share cyber risk advice and mitigation strategies.

2.4 Review and improve arrangements for sharing cyber threat intelligence with critical infrastructure and essential service providers, in partnership with Emergency Management Victoria.

2.5 Develop an annual cyber exercise program in partnership with Victoria's critical infrastructure owners and operators, to support the continuous review and improvement of Victoria's cyber emergency management arrangements.

Improve approaches to reducing the likelihood and community impacts of cybercrime

2.6 Support the delivery of a new Victoria Police Cybercrime Strategy to boost Victoria Police capability to prevent, detect, disrupt and prosecute cybercrime affecting Victoria.

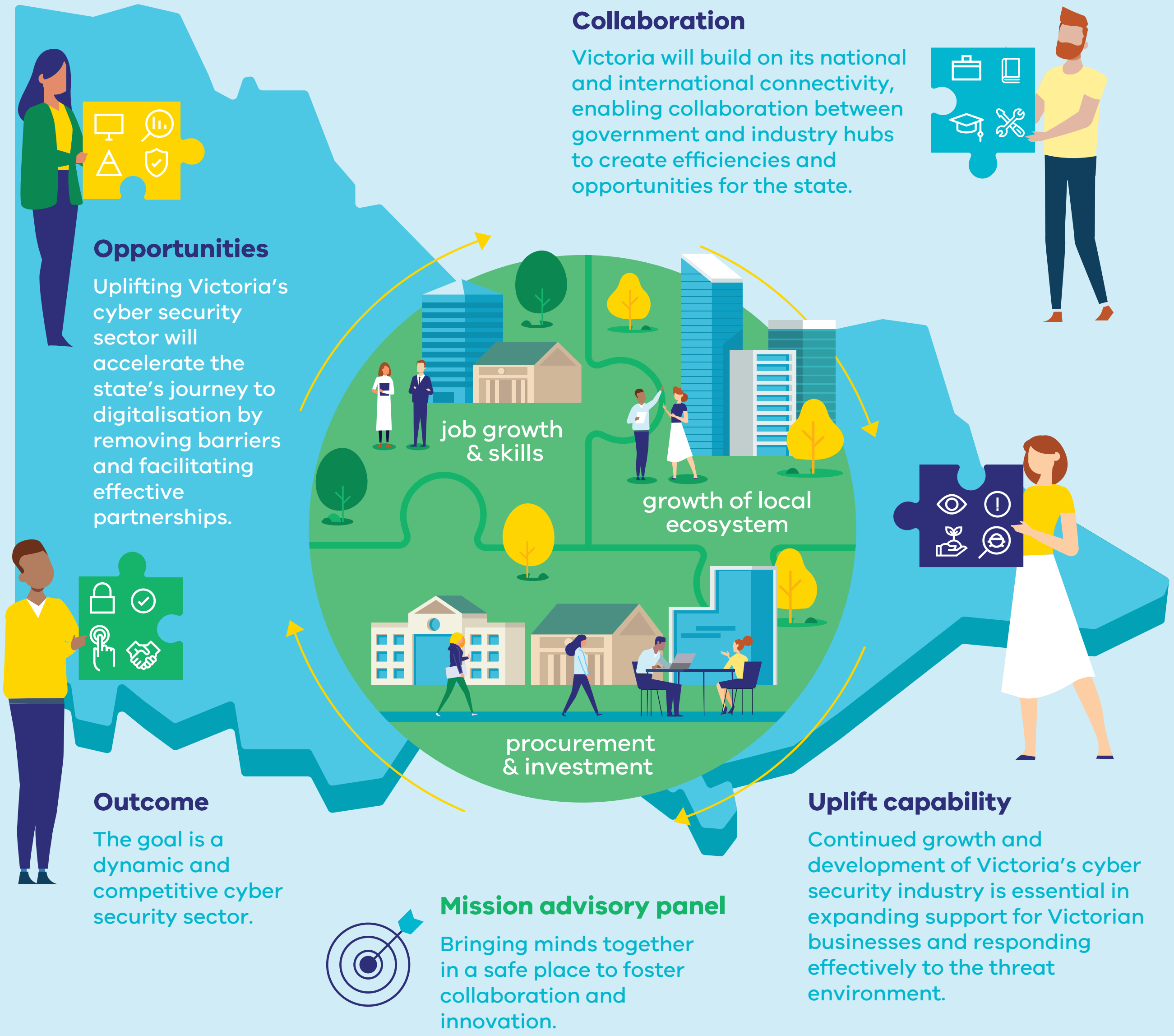
Support improved cyber resilience for government, industry and community groups

2.7 Review cyber risk messaging and education programs for government, business and community groups to identify improvement opportunities.

Mission Three

5

A vibrant cyber economy



Collaboration

Victoria will build on its national and international connectivity, enabling collaboration between government and industry hubs to create efficiencies and opportunities for the state.

Opportunities

Uplifting Victoria's cyber security sector will accelerate the state's journey to digitalisation by removing barriers and facilitating effective partnerships.

Outcome

The goal is a dynamic and competitive cyber security sector.

Mission advisory panel

Bringing minds together in a safe place to foster collaboration and innovation.

Uplift capability

Continued growth and development of Victoria's cyber security industry is essential in expanding support for Victorian businesses and responding effectively to the threat environment.

Figure 3 – Mission Three roadmap

Introduction

Victoria must develop a strong technology skilled workforce and innovative local cyber security businesses and enhance cyber resilience across all industries. Creating a vibrant cyber economy supports the growth of cyber security skills, businesses and jobs. The Victorian Government seeks to leverage the state's excellence in technology and innovation culture to position Victoria as a global leader in the growing cyber market.

Mission Three aims to develop strategic partnerships to grow a dynamic and competitive cyber sector underpinning digital transformation, growth and innovation across every sector of the Victorian economy. The mission also presents opportunities for local job creation, foreign direct investment and to improve cyber skills and expertise. These actions will position Victoria as a global leader in cyber risk management and support the state's economic prosperity.

Mission Three priorities

Growth and maturity of Victoria's cyber ecosystem

As Victoria looks to prosper in a digital economy, cyber capability and security will be instrumental in the state's economic recovery from the effects of the coronavirus (COVID-19) pandemic.

SHAKSHUKA
LABNE PLATE
Between the bread
HALOUMI & POACHED EGGS
SATAY CHICKEN
THE CUBAN
THE NEW YORKER
NEW ORLEANS MUFFULETTA
WEEKEND SPECIAL
ISRAELI BREAKFAST

The risk of malicious cyber activity is now the second highest identified state risk. As coronavirus (COVID-19) accelerates the uptake of digital business models by industry and drives a rapid shift to remote working, education and consumption patterns, it has exacerbated the threat of malicious cyber actors and made the threats more complex.

In this context, the growth of innovative, competitive local cyber security businesses and advanced capability is essential to securing Victoria's economy, reducing the community impact and harm associated with cybercrime.

Critically, these local cyber businesses will also enable Victoria to benefit from significant market and job opportunities.

The global and Australian cyber security market is growing rapidly, and Victoria is well positioned to capture a significant share of these markets. Between 2017 and 2020 global spend on cyber security products and services grew by 30 per cent. Over the last year, global spend on cyber was US$147 billion and is expected to reach US$207 billion by 2024. Australians spent $5.6 billion on cyber security over the last year and this is expected to grow to $7.6 billion by 2024. Capturing opportunities in cyber could create thousands of skilled, high value job opportunities over the next few years, adding to the almost 27,000 workers employed in cyber security roles in Australia today.

Internationally recognised training and development programs with established pathways into cyber employment

The growth of competitive cyber firms and development of cyber awareness and resilience across the economy relies heavily on access to high level skills and expertise to meet evolving demands.

The coronavirus (COVID-19) pandemic escalated Victoria's shift to online working, studying and entertainment. It has highlighted the critical importance of access to a workforce skilled in technology and creating demand for digital and cyber security skills across our economy.

Further strengthening those skills will benefit industry by expanding the pool of local digital talent and create opportunities for Victorians to move into new careers.

3. AustCyber Report 2019

Increased investment opportunities and industry maturity

Stronger industry cyber capabilities are enablers of digital economic growth. They facilitate access to security sensitive global supply chains and underpin Victoria's investment value proposition, opportunities for jobs growth and the economic recovery across priority industry sectors.

There are significant opportunities for development of the cyber ecosystem through key industry sectors including

- advanced manufacturing
- medical technologies and pharmaceuticals
- professional services
- agriculture (food and fibre) and
- defence technologies

Attracting the presence of international cyber and technology companies to invest and operate in Victoria will enhance the capabilities of our local cyber start-ups and small business sector and provide opportunities to support and partner with Victoria's leading fast growing cyber product and services ecosystem.

Target state

The Victorian Government will foster the building of strategic partnerships to accelerate the state's further transition towards online delivery, removing potential barriers to adopting digital technologies by government, and facilitating partnerships with industry, universities and research institutes.

The government will support the growth of a steady local pipeline of cyber talent by strengthening its focus on university and vocational cyber security training programs, mid-career re-training/upskilling, attracting expats and skilled migrants and coordinating their alignment with industry needs and global trends. This includes skills and talent in areas such as technical, risk, education, analytics and administration.

It will also facilitate pathway opportunities into industry and government roles.

Victoria will build on its national and international connections, relationships and agreements to promote collaboration between government and industry creating efficiencies and opportunity for the state.

The Victorian Government will promote cutting-edge cyber technology solutions, and actively procure local capability where possible. It will also assist Victorian cyber companies to scale and export their services and products successfully.

In so doing, we will increase the attractiveness of the state as a place for established technology companies to invest, driving revenue and strong international investment.

Actions

Grow local capability

3.1 Establish an Expert Advisory Panel to provide insight on current and future cyber capability uplift opportunities and digital economic growth

The Expert Advisory Panel will aim to report to government on:

a. skills and capabilities required in current and key future growth sectors

b. opportunities to influence and leverage Commonwealth and State initiatives, uplifting small business cyber security

c. opportunities to drive enhanced business engagement with the cyber ecosystem, to safeguard and underpin our current and future growth sectors

3.2 Collaborate with AustCyber to map Victoria's cyber security ecosystem and understand local capabilities

3.3 Support the cyber security awareness and capabilities of SME's through Small Business Victoria's suite of support programs

3.4 Explore opportunities for Victorian cyber start-ups to access developmental support and capital, through LaunchVic and Invest Victoria's suite of support programs

3.5 Strengthen support for investment in research, innovation and commercialisation of cyber-security technologies

Enhance cyber skills development, pathways into employment and job growth

3.6 Support the growth of Victoria's cyber industry and boost advanced digital technology industry skills through the Cremorne Tech Hub

3.7 Provide cyber skills and facilitate internship opportunities to lift the participation of Victorians in digital careers

3.8 Establish an internship program to support more women into senior leadership roles in the cyber sector

3.9 Continue to support university and vocational training cyber security programs to build cyber skills and capability

3.10 Work across government to facilitate a whole of Victorian Government Cyber Certificate IV Internship Program

Support industry maturity and investment opportunities

3.11 Foster opportunities for leading Victorian cyber security SMEs to partner with global technology firms that invest, operate and locate in Victoria

3.12 Support Victorian exporters to better understand and manage their cyber security risks when operating in global markets

3.13 Identify opportunities to accelerate cyber-secure industry standards and practices through key business and technology precincts

Delivery partners

6

Effective reduction in harm from cyber-attacks requires collaboration across government, industry and the community. Cyber risk knows no boundaries and does not adhere to jurisdictional or geographical borders.

The Victorian Government recognises that strong domestic and international partnerships, spanning government, industry and the community, are essential to successfully delivering Victoria's Cyber Strategy 2021.

Victorian Government

The Victorian Government is a collection of over 1,800 agencies that hold unique capabilities and provide a variety of services and contact points to the public. This strategy will leverage the collective capability of all Victorian Government agencies to deliver on our three core cyber safe missions.

Government partnerships

Australia's national, state and territory governments recognise the interconnected nature of cyber risk and its effect on Australia's national interests.

The Victorian Government will remain a key participant in the National Cyber Security Committee, contributing to the development of national cyber risk management strategies and related capabilities.

We will advocate and prioritise joint cyber investments with other states, territories and the Australian Government wherever practical. It is important to reduce the cost of cyber security to government and reduce cost and complexity of businesses to provide services to government.

Industry partnerships

Cyber safety is a highly evolving field with continual new thinking occurring both in industry and government. Sharing this knowledge and capability is beneficial for Victoria.

The Victorian Government will improve knowledge sharing with industry and improve procurement practices to allow for faster engagement with industry when support is required.

Additionally, we will engage with commercial entities, not-for-profit organisations and industry associations that seek to contribute to society by providing philanthropic goods and services, including cyber-related services. We will work with these organisations to ensure the benefits of their activities are maximised for all Victorians.

Academic partnerships

Victoria is renowned for the quality of its academic institutions. The Victorian Government will work with local academic institutions to help create a cyber smart population and continue to be a world leader in cyber research.

> The Victorian Government will improve knowledge sharing with industry and improve procurement practices to allow for faster engagement with industry when support is required.

VICTORIA
State
Government