Cyber Threats & Resilience

PROV Records Management Network

28th March 2023

VICTORIA State Government

Cyber Threat Landscape

Response

Victorian Cyber Strategy

Insight from Recent Breaches

Future

VICTORIA
State Government

Cyber Threat Landscape

- We have experienced a rapid shift to remote work and online service delivery
- Global - US$6T 2022, US$10.5T 2025
- National - $33B self reported losses 2020/21 (2% GDP). Australians lost >$300M to spam in 2020/21
- Our treat actors range from annoying, through to well organised cyber crime groups to highly sophisticated and well-resourced nation states
- The level of threat we face from foreign espionage and interference activities is currently unprecedented
- Increased likelihood of cyber-attacks impacting critical infrastructure, service delivery and public confidence

Cyber Threat Landscape

- Cyber criminals target government, industry, business and the community. No one is immune. Cyber attack reported to ACSC every 7 mins (76K in 2021/22 - Vic 27%).

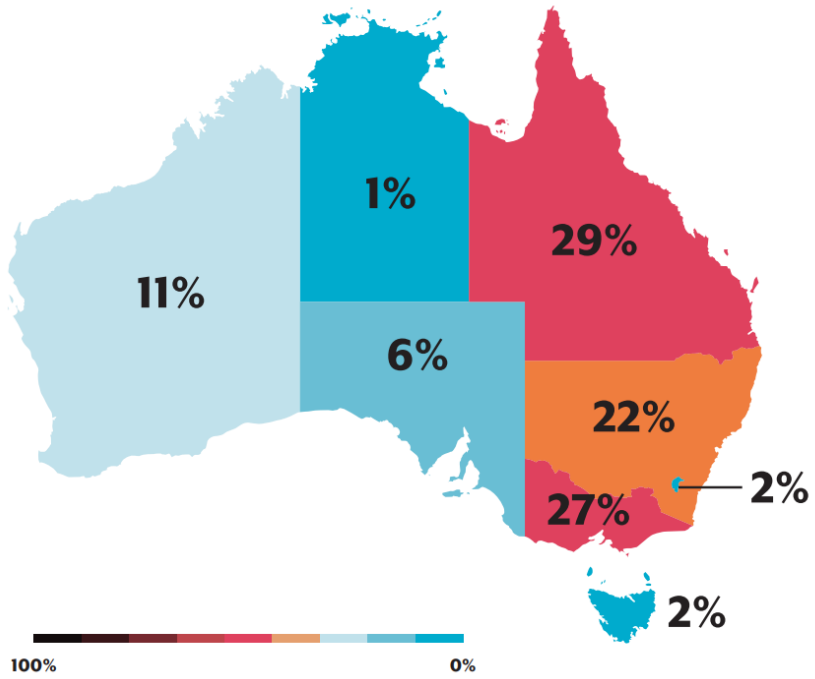


Figure 2: Breakdown of cybercrime reports by assigned jurisdiction for financial year 2021–22

ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au

Response

VICTORIA
State Government

What are we doing

- **Cyber Governance and Metrics** - departments and agencies are accountable for managing cyber risks within their department and portfolio entities. Cyber is a business risk. Integrate cyber threats into existing risk management frameworks and processes

- **Cyber Culture** – stakeholders need to be aware, but they also need to care enough to take action (stakeholder briefings, training, communication)

- **Cyber Maturity & Controls** – baseline controls are not adequate. Promote ASD/ACSC Essential 8 which will prevent or limit impact of up to 85% of current cyber incidents. Commenced Sept 2020. https://www.vmia.vic.gov.au/cyber-maturity-benchmark

- **Asset Management** - need much better visibility of assets supporting critical services, existing and emerging vulnerabilities, and detecting anomalous activity

- **Threat Intelligence** – leverage, enhance, action, and assurance

- **Guidance & Advice** – strategy, policy, patterns, standards, guidelines, secure by design, secure by operation

Cyber Strategy 2021 overview

VICTORIA
State Government

Strategy overview

Vision: to create a cyber safe Victoria

Over the next five years, the strategy will continue to harness opportunities for Victoria to collaborate across government, industry and the community to support local cyber businesses, developing a dynamic and competitive cyber sector underpinned by innovation and jobs growth.

The Victorian Government Chief Information Security Officer (CISO) will release annual Mission Delivery Plans that outline specific activities associated with the three core missions identified in this strategy.

For more information and to download the strategy visit www.vic.gov.au/cyber

https://youtu.be/_g63pySWSGE

Vision: Cyber Safe Victoria

Mission 1

19 x MDP actions

The Safe and Reliable Delivery of Government Services

- Protecting Victorian Government services, networks and data
- Improve baseline controls, governance and assurance
- Strengthening the resilience of essential services

Mission 2

7 x MDP actions

A Cyber Safe Place to Work, Live and Learn

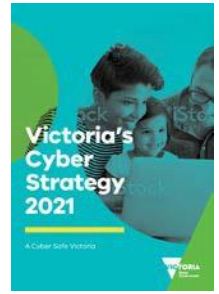
- Improve understanding of cyber risk, issues and community response opportunities
- Support Victoria's small business community, critical infrastructure and essential services

Mission 3

15 x MDP actions

A Vibrant Cyber Economy

- Grow local capability
- Enhance cyber skills development, pathways into employment & job growth
- Support industry maturity and investment opportunities



Recent Cyber Attacks

VICTORIA
State Government

The Future

VICTORIA
State Government

The Future

- Scale and pace of digital transformation
- Increased cyber hostility
- More and larger data breaches - assume breach
- Critical infrastructure and OT, and 3rd party (supply chain) compromise
- Accountability and consequences for cyber attacks
- Demand continues to outpace supply of capable cyber resources
- Automated defence and attack
- Think differently

Attachments

VICTORIA
State Government

Achievements – protecting government systems

Mission One: **The safe and reliable delivery of government services**

Achievements:

- Recognition of risk and acceptance of need for change
- Responded to >950 cyber incidents from >180 govt entities. Services include threat intel and alerts, WoVG incident co-ordination, exercises.
- Cyber Security Benchmark – E8 with VMIA
- Sector uplift, sector SOCs, and sector CISOs
- Email Trust Program - DMARC
- Cyber Security Architecture Practice
- 3rd Party Risk Management Program

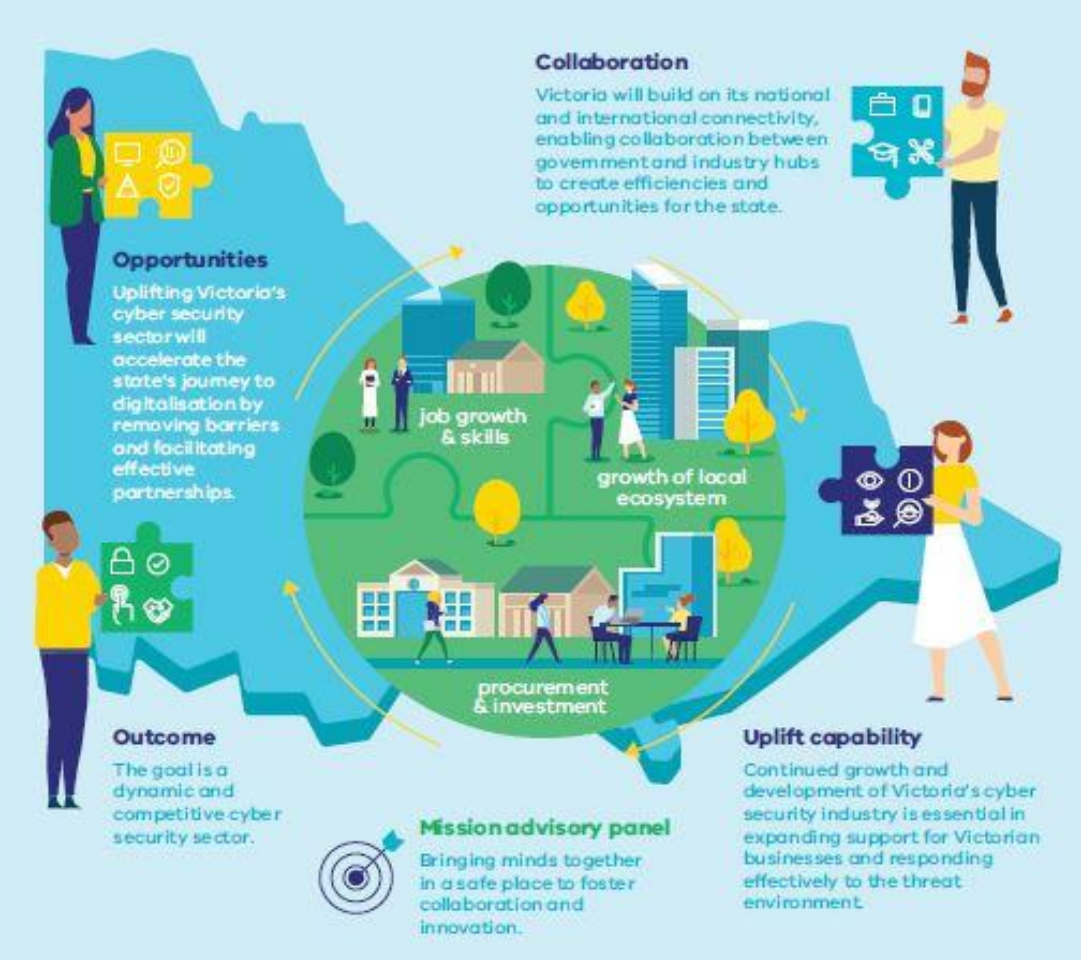
Achievements – protecting the community

Mission Two: **A cyber safe place to work, live and learn**

Achievements:

- Expert Advisory Panel
- Australian Institute of Criminology study on cybercrime in Victoria. Supporting Victoria Police Cybercrime Strategy to prevent, detect, disrupt and prosecute cybercrime
- SME resilience, community messaging and schools engagement

Achievements: growing Victoria's cyber sector



Mission Three: **A vibrant cyber economy**

Achievements:

- Expert Advisory Panel
- Cyber skills pathways – Women in Security Pilot Program with AWSN, ADF Veterans, early and mid-career interns
- Support for local cyber industry and start-ups
- Attracting global organisations to establish a presence in Victoria

Jobs, Precincts and Regions

Premier and Cabinet