VICTORIA State Government | Government Services

PROGRESS TO DELIVER VICTORIA'S CYBER STRATEGY

Delivering a Cyber Safe Victoria

This is the first annual statement by the Victorian Government Chief Information Security Officer on the progress to implement Victoria's Cyber Strategy.

The cyber threat environment in Australia continues to grow in scale and complexity. Three years ago, the Australian Cyber Security Centre released landmark statistics indicating that a new cyber-attack was reported in Australia every 10 minutes. Fast-forward to 2022, and the time between cyber-attacks has reduced to 7 minutes, with almost one-in-four of these attacks causing harm to someone in Victoria.

Late 2021, the Victorian Government released Victoria's Cyber Strategy, backed by a $50.8 million investment. The five-year strategy sets the government's vision for creating a cyber safe Victoria, a place where government, industry and the community can connect and deliver services safely and securely online.

We are delivering the strategy with a focus on three core missions:

- Improving the safe and reliable delivery of government services
- Creating a cyber safe place to work, live and learn
- Supporting a vibrant cyber economy.

In the first year of delivery, we have heavily focused on building the solid foundations and partnerships across government and industry that are required to see the strategy succeed over the next four years.

We kicked off this work by launching programs to strengthen the protection of our critical services and defend against common cyber-attacks. By promoting the adoption of the Australian Signals Directorate's Essential 8 maturity model across government, we are effectively mitigating common cyber-attacks and protecting personal and sensitive information. We also strengthened the cyber security of the government supply chain by improving government's approach to procurement of goods and services, while also educating government organisations on the safe and secure use of cloud technology.

Bolstering the Victorian Government's ability to detect and respond to new and emerging cyber risks, we established the first of our new Security Operations Centres, introduced automated threat intelligence sharing programs, and strengthened resources for the Victorian Government Cyber Incident Response Service.

Through widespread implementation of Domain-based Message Authentication, Reporting and Conformance (DMARC) capability across email services using the vic.gov.au domain, we have also improved the protection and integrity of public sector digital services.

Staff training and education has been a key feature of our work. Staff across the public sector have been educated to identify and respond to potential cyber risks. Staff in high-risk and sensitive roles have been supported to enhance protection of security classified and sensitive information against unauthorised access. Training has also been provided to members of government boards so they can better understand and fulfil their cyber security obligations.

The cost of cybercrime on Victorian businesses and community members is both significant and rising. The Australian Cyber Security Centre reports the average cost per breach in Australia is $39,000 for small business, $88,000 for medium business, and over $62,000 for large business – an average increase of 14%. The toll on individuals is also significant, with major privacy breaches increasing the potential for fraud and identity crime across the community.

We established Victoria's first Expert Advisory Panel on Cybercrime to improve cyber protection for Victorian businesses and the community. It brings together leading cyber figures from government, industry, academia, and victim support services to provide tailored advice to government to help shape policy and decision making. This panel contributed to a comprehensive report on cybercrime in Victoria by the Australian Institute of Criminology, a report which helped shape the first 12-months of delivery of the Cyber Strategy.

The Department of Jobs, Skills, Industry and Regions also established an expert advisory panel to help us boost Victoria's cyber sector. The panel considered opportunities for building sovereign capabilities, sector scale and maturity, boosting cyber security awareness and capabilities, strengthening Victoria's reputation as a hub for cyber entrepreneurs, and strengthening Victoria's cyber ecosystem—including support for small and medium businesses.

I would like to thank everyone who contributed to the success of these panels.

By building strategic partnerships with private industry and academia, we are growing a dynamic and competitive cyber sector. The Victorian Government's Free TAFE initiative is now providing Victorians looking to enter the cyber security workforce with free access to a Certificate IV in Cyber Security. This accredited and nationally recognised course is offered at 19 locations around Victoria. It provides the knowledge and skills to work in cyber security jobs.

The Victorian Government is also creating new job opportunities and pathways through our partnerships with programs such as Code Like a Girl, the Australian Women in Security Network, Digital Jobs Program, and the Neurodiverse Talent Entry Program. These programs helped Victorians to transition into the cyber and digital workforce, and provided hands-on experience through internships in industry, as well as with Digital Victoria and other public sector bodies.

Looking ahead, I am pleased to release our next mission delivery plan and share the strategic initiatives and priorities that guide our future delivery of Victoria's Cyber Strategy. This plan reflects the dynamic nature of the cyber security environment and highlights our adaptive approach towards building a cyber safe Victoria.

Victorian Government Chief Information Security Officer

Department of Government Services

17 February 2023