CAPTURA CYBER | CLARITY IN CYBERCRIME EVIDENCE

29 August 2025
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100 Parliament House
Canberra ACT 2600

Submission to the Parliamentary Joint Committee on Law Enforcement Inquiry into the Capability of Law Enforcement to Respond to Cybercrime

Dear Secretary,

Captura Cyber is a provider of cybercrime investigation as well as training and development for public and private-sector organisations. Captura Cyber delivers cybercrime investigation and capacity building in Australia and internationally.

Challenges in responding to cybercriminal activity are well established: cybercrime crosses international boundaries, making it challenging for law enforcement to investigate and prosecute locally. Cybercriminals constantly adapt to new technologies and develop sophisticated methods to evade detection. Encryption and anonymity make it difficult for law enforcement to trace cybercriminals and to gather evidence. Criminal use of cryptocurrencies poses particular challenges for law enforcement.

This submission outlines the specific training requirements we believe Australian law enforcement requires to respond effectively to cybercrime.

Nationally Standardised Cybercrime Training

Other Five Eyes nations have fundamentally stronger law enforcement capabilities for identifying, investigating and responding to cybercrime. While approaches vary in the USA, Canada, and the UK, each country provides their law enforcement agencies with centralised, coordinated and standardised cybercrime training. This ensures that smaller, less well-resourced agencies have access to the same training and resources as larger agencies.

In the USA, cybercrime training offered by federal agencies such as the FBI and the Department of Homeland Security on centralised platforms covers areas including electronic law, evidence collection, and investigative techniques.

The Canadian Police College offers centralised and nationwide advanced courses to all law enforcement agencies in the country. Training in digital forensics and cybercrime investigations is delivered by law enforcement and private sector experts.

In the United Kingdom, the National Cyber Security Centre (NCSC) Assured Training scheme is a standards-based framework, that is a prime example of centralisation through quality control rather than direct provision. The National Police Chiefs' Council also works across law enforcement agencies to develop resources and tools to tackle cybercrime, further contributing to a nationally coordinated effort.

Conversely, the Australian law enforcement cybercrime training model is demonstrably non-centralised and fragmented, despite the existence of a central coordinating body.

Recommendation:
Australia establishes centralised and standardised cybercrime training, comparable to models used in the USA Canada and the United Kingdom.

Cybercrime Training for Police Recruits

In 2023/2024 ASD received over 87,000 reports of cybercrime over the financial year, an average of a report every six minutes.

Responding to cybercrime is now a core business for law enforcement organisations. Traditionally, cybercrime response has been regarded as a niche area within law enforcement handled by specialised units.

Instead, new frontline staff should be trained in how to respond, to document, and to preserve digital evidence. This is consistent with a recommendation of the 2022 UK House of Commons Justice Committee inquiry into 'Fraud and the Justice System', that all law enforcement recruits receive training in digital crimes, including cyber-enabled fraud. Uplifting organisational capacity in this way is supported by other Australian and international research.

Recommendation:
Australian federal and state law enforcement agencies implement foundational cybercrime awareness training for frontline staff (often known as recruit or cadet training).

Executive Education in Cybercrime Leadership

As a relatively new and evolving crime type, many law enforcement executives have no experience managing cybercrime, but are responsible for developing cybercrime policies and protocols, leading public/private partnerships, and resourcing cybercrime investigations.

The Australian Institute of Police Management, which provides executive development programs for senior officers of all police services in Australia and New Zealand, currently offers no programs in cybercrime leadership.

Education for organisational leaders would empower executives with an overview of the cybercrime landscape, its unique characteristics, resourcing requirements, and investigative challenges.

Recommendation:
Incorporate cybercrime education into executive leadership programs to equip law enforcement executives to lead agile organisations that can respond effectively to escalating rates of cybercrime.

Conclusion

Implementing the above recommendations would achieve two outcomes

- Strengthen the cybercrime response capability of law enforcement agencies throughout Australia.
- Signal that Australia is no longer a "soft target"[1] for cybercrime threats.

We would be pleased to discuss these matters further with the Inquiry.

[redacted]

Garren Hamilton

Managing Director

Captura Cyber Pty Ltd

29 August 2025

[1] Parliamentary Joint Committee on Law Enforcement - Cybercrime Inquiry Public Hearing 23/05/2024 - Hansard p.27