Australian Banking Association

Submission to Joint Parliamentary Committee on Law Enforcement

15 December 2023

Australian Banking Association

Context

The ABA welcomes the opportunity to respond to the Joint Parliamentary Committee's inquiry into the capability of law enforcement to respond to cybercrime.

Cybercrime's complexity exemplifies a wicked problem – it is a challenge that resists solutions, cannot be solved in a single domain only, and where a critical part of any solution (technology), is perversely also an enabler. In Australia, cybercrime has become a pervasive and persistent threat to individuals, businesses, and government, while Australia's high level of technology adoption and relative wealth makes it an enduringly attractive target for cybercrime.[1]

As the ever-growing reliance on technology in society further converges the lines between our physical and digital lives, cybercrime threats and subsequent demands on law enforcement will continue to grow. This challenge is particularly prevalent in the asymmetric nature of threat actors – a lone actor anywhere in the world can instigate an attack – while the blurred lines of attribution between jurisdiction, criminal and commercial law, and the state means solutions are illusive and criminals have no shortage of opportunities to exploit. The summation of these challenges and the inherent limitations on legislative and regulatory controls necessitate society-wide cooperation and a relentless pursuit of opportunities to enhance the capacity of law enforcement to respond.

Law enforcement has deep expertise and is highly engaged in cybercrime.

The ABA recognises the substantial expertise and capability already employed by Australian law enforcement in the disruption and response to cybercrime including the AFP/ASD led Operation Aquila, and the ASD's Project REDSPICE. The continued focus of the Commonwealth Government is welcomed, with the 2023 Cyber Security Strategy providing a promising framework for nation-wide cooperation in keeping Australians safe. The ABA looks forward to further engagement with government and industry as the strategy progresses.

Reflecting the initial open-ended nature of this inquiry and the substantial policy work currently underway, the ABA has used this consultation as an opportunity to highlight opportunity areas with direct implications on the response capacity of law enforcement. There is no panacea in addressing cybercrime, however these areas – jurisdictional complexity, intelligence sharing, and individual and businesses cyber resiliency – illustrate the unique challenges of enforcing the law with respect to cybercrime and represent vital responses to support law enforcement efforts.

Policy Director contact:

Policy Director

About the ABA

The Australian Banking Association advocates for a strong, competitive, and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

[1] Australian Cyber Security Centre 2022

Australian Banking Association

Domestic jurisdictional complexity

Australia's domestic[2] legal framework affirms the application of standard geographical jurisdiction in cybercrime cases; however, the borderless nature of cybercrime means that no Australian jurisdiction can effectively tackle cybercrime in isolation. Traditional policing – based on territoriality – has its efficacy limited by the ubiquity of the internet as the traditional nexus between the geographical locations of the criminal and victim/s has been severed. These complications become particularly noticeable under circumstances where cybercrime statutes differ, offenders relocate to a third jurisdiction, where an offender's nationality differs from their geographical jurisdiction, victims are in multiple jurisdictions, or where evidence is stored across multiple jurisdictions.

The cybercrime business model – increasingly a value chain of specialised functions – involves an ecosystem of offences from sophisticated cyber-attacks to monetisation through fraud and scams. Concurrently, the growth of cryptocurrency and digital assets has greatly expanded the capacity for downstream financial crime to be executed off the back of cyber and fraud crimes. The jurisdictional authority and capability to respond to this ecosystem meanwhile is dispersed across state police, the AFP, and federal agencies, creating ambiguity and friction in responding to the entire value chain of cybercrime.

For example, while computer intrusion cyber offences are often a precursor to fraud, these offences – legislated under both state and federal laws – generally carry much lower penalties than state-based fraud crimes and are more difficult to prosecute, prioritising enforcement resources towards the fraud component of the value chain.[3] While states have been proactive in establishing specialised cyber-policing units, generally speaking most cybercrime capabilities rest with the AFP. Variation in legislation and law enforcement powers across states furthers this challenge – e.g. Victoria Police have powers to seize cryptocurrency and digital assets, while other jurisdictions are more limited. In the context of jurisdiction and varying state police capabilities and resourcing, this paradigm has the potential to drive divergent outcomes of cybercrime enforcement in different states.

Opportunities

Law enforcement initiatives have sought to adapt to jurisdictional complexities. The Joint Policing Cybercrime Coordination Centre (JPC3) is a notable example, bringing together all Australian policing jurisdictions, coordinating counterresponses and facilitating capability uplift. To supplement and enhance this work, ongoing attention should be given to:

- Identifying opportunities for greater operational and legislative harmonisation between states and the Commonwealth. This would support greater holistic responses to the cybercrime business model. E.g., enforcement over identity fraud must address the intrusion of data, the perpetration of fraud, and the downstream financial benefits gained from fraud.
- Expanding state police cybercrime expertise, reflecting the salience of cyber enabled crimes like scams and identity fraud, which are experienced locally at the individual and community level and are generally investigated by state police.

[2] International jurisdictional issues have been intentionally omitted from this submission.
[3] Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims.

Australian Banking Association

Barriers to information sharing

Effective disruption of cybercrime necessitates efficient intelligence sharing between law enforcement and industry, including banks, telcos, and digital platforms. With 1 in 5 critical cyber vulnerabilities being exploited within 48 hours[4], timely and reliable information flows are critical. There are naturally necessary limitations on intelligence sharing, however other asymmetries and incomplete information can inhibit both prevention efforts and the capacity of industry to support the law enforcement response. These asymmetries are multi-directional, including intelligence flows to government, from government, and industry-to-industry.

There are many barriers to more open information sharing from industry, including perceived risk of regulatory action, potential legal action, and reputational risk. The intersectionality of compliance obligations with cyber (e.g. privacy) can further propagate reluctance to disseminate useful intelligence. While government agencies (i.e. the ACSC, ASD, AFP) – at the forefront of threat vector analysis – already facilitate models of intelligence sharing from government to industry, there are often limitations to the timeliness and accessibility of real-time intelligence.

Opportunities

The 2023 Cyber Security Strategy demonstrates alertness to the need for greater multi-directional intelligence flows. The strategy outlines the rationale for policy reform to enable greater industry-outward sharing including a 'no fault, no liability' ransomware reporting proposal and a proposed 'limited use obligation' that clarifies how the ASD, and the cybersecurity coordinator may use cyber incident reporting.[5] Intelligence from government-to-industry and industry-to-to industry threat intelligence is already active through the ASD's intelligence threat sharing platforms and the Cyber and Infrastructure Security Centre's Trusted Information Sharing Network. This model works well, however as identified in the 2023 Cyber Security Strategy, the velocity of threat vectors is increasing, requiring ongoing uplift in intelligence sharing practices.

The ABA supports practical steps to improving industry wide disclosure confidence and more timely dissemination of useful intelligence. Improving the quality and quantity of useful information requires continued focus on:

- Responsibly simplifying and de-risking the sharing of information from industry to government. Attention should be given to navigation challenges where conflicting compliance obligations like privacy legislation can create unintended barriers to timely incident responses.
- Developing with key sectors models for greater economy-wide intelligence sharing between industry, government, and law enforcement. While existing industry models exist, deeper multi-sector cooperation recognises that cyber threats are not isolated to single industries.

Individual and business cybercrime resiliency

Malicious actors are incentivised to attack individuals and smaller businesses as their relative vulnerability and centrality to the cybercrime business model makes them appealing targets. These criminals go to great lengths to steal identities and personal data of Australian citizens, including through large-scale breaches of businesses holding personal customer data. This data is

[4] ASD Cyber Threat Report 2022-2023
[5] 2023 Cyber Security Strategy

Australian Banking Association

commoditised, then on sold to others to be leveraged for downstream offences like fraud and scams. This allure extends to small and medium businesses – often lacking the resources and capabilities of large corporations and governments.

As the first line of defence against cybercrime and wider economic disruption, both uplifting the capability of individuals and businesses to respond to cybercrime, and minimising the opportunities for exploitation are critical. While the economic impact alone of cybercrime is substantial – totalling $3.5b for individuals[6] and averaging $46,000 and $97,200 for small and medium business respectively[7] – cybercrime incident volumes strain law enforcement resources.

Despite this centrality, cyber awareness remains a challenge in the community, and for many, understanding advice on how to remain safe is hard to navigate. Networks of cybercriminals are sophisticated, constantly innovating in tactics, so that the community is often unaware of current vulnerabilities and threats. At same time, most cybercrime remains unreported – less than 20% of victims seek help from police or use Reportcyber[8] – and many Australians don't know how to seek support when they are targeted. These barriers can perpetrate a cycle of stigma, prolonging the impact of cybercrime. While often necessary, data retention practices and customer identification obligations on businesses incentivises cyber-attacks against them.

Opportunities

The ABA supports the 2023 Cyber Security Strategy's call for greater action to address these issues, including recognising the challenges posed by data holding requirements on businesses. Government, law enforcement, and industry have long been responsive. Cyber awareness campaigns, and police community engagement builds greater community resiliency, while continuous uplifts of control environments (e.g. authentication) reduce opportunities for cybercriminals. The introduction of a single reporting tool to streamline incident reporting is welcomed, however many individuals and businesses remain unaware of this and still have difficulty in using it.

The ABA supports continued momentum on the below opportunity spaces identified in the 2023 Cyber Security Strategy as instrumental in reducing both impact of cybercrime on Australians and the burden on law enforcement.

- Continue development towards a Digital ID program to reduce the need for people to share sensitive personal information with businesses to access services online. This will mean fewer records of individuals' ID data and documents held by businesses – reducing the risks of identity theft, the impact of fraud, and the appeal of businesses as cybercriminal targets.
- Facilitate comprehensive multi-industry engagement on enabling technologies – particularly across telecommunications services, internet service providers, and digital platforms (e.g. social media) – to limit more cybercriminals from reaching their intended targets and block threats at scale.
- Incorporate greater cybercrime education into public crime prevention engagement. Initiatives like Crime Prevention Weeks run by police across all states uplift community resiliency, however, these predominantly focus on traditional crime, with cybercrime education often very limited.

[6] Australian Institute of Criminology 2023
[7] ASD Cyber Threat Report 2022-2023
[8] Australian Institute of Criminology 'Cybercrime in Australia 2023'.