Parliamentary Joint Committee on Law Enforcement

Inquiry into the capability of law enforcement to respond to cybercrime

Submission by the Australian Securities and Investments Commission

December 2023

Contents

Submission by ASIC

1 On 16 October 2023, the Parliamentary Joint Committee on Law Enforcement agreed to inquire into and report on the capability of law enforcement to respond to cybercrime, including:

(a) Existing law enforcement capabilities in the detection, investigation and prosecution of cybercrime, including both cyber-dependent crimes and cyber-enabled crimes.

(b) International, federal and jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats.

(c) Coordination efforts across law enforcement, non-government and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime.

(d) Emerging cybercrime threats and challenges affecting Australian entities and individuals, including the scale and scope of cybercrimes conducted in Australia or against Australians.

(e) The opportunities and challenges of the existing legislative framework in supporting law enforcement to investigate and act upon instances of cybercrime.

(f) Prevention and education approaches and strategies to reduce the prevalence of victimisation through cybercrime.

(g) Other related matters.

2 This submission focuses on (c), (d) and (f) of the terms of reference. Specifically the limitations of existing information-sharing arrangements around cyber threat intelligence and cyber incidents and how this impacts the performance of ASIC's statutory duties, including enforcement action.

3 The interconnected nature and criticality of financial markets and services means that timely intelligence sharing at the outset of a cyber incident is vital to maintaining the integrity of Australia's financial system. Prompt incident response coordination and consequence management ensures an efficient response that minimises harm to consumers and the risk of systemic disruption.

4 Visibility over vulnerabilities and intelligence from the outset is essential to ensure ASIC can act quickly to fulfil its obligations as regulator by managing the consequences and broader impact of a cyber incident on Australia's financial and corporate sectors. This does not include an evidence-gathering exercise for future regulatory action.

Introduction and background

5 ASIC is established under the *Australian Securities and Investments Commission Act 2001* (ASIC Act). ASIC is Australia's corporate, markets, financial services and consumer credit regulator.

6 The ASIC Act requires that in performing its functions and exercising its powers, ASIC must (among other things) strive to:

(a) maintain, facilitate and improve the performance of the financial system and entities in it;

(b) promote confident and informed participation by investors and consumers in the financial system; and

(c) take whatever action we can, and which is necessary, to enforce and give effect to the law.

7 ASIC is committed to maintaining market integrity and supporting fair and efficient markets that investors and consumers can participate in with confidence. We do this by regulating corporations, financial services and credit; conducting surveillances; making market integrity rules; assessing the operation of critical market infrastructure; and taking enforcement action.

8 In March this year, new ASIC market integrity rules commenced aimed at promoting the technological and operational resilience of securities and futures market operators and participants. ASIC introduced these rules in 2022, following public consultation, to enhance the resilience of Australian markets. Enforcing breaches of these rules is an identified priority for ASIC in 2024. These rules reflect the criticality of these services.

9 ASIC's *Corporate Plan 2023-24* identifies cyber and operational resilience as one of ASIC's key strategic priorities. The plan commits ASIC to active supervision and engagement with stakeholders to encourage prompt management of operational risks, and continuous improvement of cyber and operational resilience practices. It also states that ASIC will take enforcement action where there are egregious failures to mitigate the risk of cyber attacks.

Mandatory reporting framework for reporting cyber incidents to ASIC

10 ASIC-licenced entities impacted by a cyber incident should consider their licence obligations, including whether the circumstances surrounding the incident meet the threshold for a reportable situation: see Table 1 of Regulatory Guide 78 *Breach reporting by AFS licensees and credit licensees*. Where a reportable situation has arisen, the entity must lodge a report with ASIC within 30 days of the matter being identified.

11 Entities licenced by ASIC should carefully consider conduct obligations as they relate to consumers who may be affected by a cyber incident. Licensees' communications to consumers following a cyber incident should also be managed through this lens.

12 The earlier referenced amendments to the ASIC market integrity rules require market operators and participants to notify ASIC immediately upon becoming aware of a major event, which may include a cyber incident. A written report to ASIC must follow within seven days of the notification.

13 Market operators also have increased obligations to notify ASIC:

(a) immediately upon becoming aware of a disruption to critical business services that may interfere with the operation of a market; and

(b) immediately (and no later than 72 hours) after becoming aware of unauthorised access or use of critical business services or market-sensitive, confidential or personal information.

14 Market operators must have adequate arrangements to ensure the confidentiality, integrity and availability of information obtained, held or used.

15 ASIC considers these reporting streams for the purposes of consequence management during incident response – as well as to identify and understand where egregious failings to appropriately manage these risks may have occurred.

16 The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) defines consequence management as the second and subsequent order effects from cyber security incidents. Consequence management requires government and industry to work together to identify and mitigate the secondary harms that may result from a cyber incident.

ASIC's approach to incident response coordination

17 ASIC monitors disruptive cyber attacks through our regulatory teams, reporting obligations, compliance contacts and ransomware monitoring. When a regulated entity is attacked, ASIC follows relevant response plans classifying the incident. This involves considering the potential for consumer or investor harm, or whether there is significant systemic risk to financial services or markets.

18 Depending on the incident classification, ASIC may implement various industry response plans at an agency level, or together with domestic or international peer financial regulators (e.g. through the Council of Financial Regulators (CFR) or the Trans-Tasman Banking Council (TTBC)).

19 When ASIC contacts an organisation in response to an incident, we are seeking to:

(a) coordinate engagement across a number of regulators to reduce regulatory touch points;

(b) understand and act to manage any broader systemic impacts arising from the incident;

(c) raise consumer and investor considerations, such as communications, to support impacted parties in taking appropriately-informed action;

(d) engage with an entity to assist with their regulatory compliance where systems may be impacted for a prolonged period; and

(e) support recovery and understand how the incident occurred.

20 Incident response coordination and consequence management is about minimising the potential harm, including systemic disruption – it is not about compiling evidence for future regulatory action.

ASIC's approach to law enforcement

21 Consistent with our strategic priorities, ASIC has previously taken enforcement action in relation to cybersecurity risks in proceedings ASIC filed against RI Advice in the Federal Court of Australia. In that case, the Federal Court found Australian financial services licensee, RI Advice, breached its licence obligations by failing to act efficiently and fairly, and by failing to have adequate risk management systems in place to manage its cybersecurity risks. The finding came after a significant number of cyber incidents impacted authorised representatives of RI Advice between June 2014 and May 2020.

22 ASIC is, and will continue to, assess information it receives about cyber incidents to determine whether enforcement action is appropriate where there are egregious failures. ASIC is actively considering such matters at the time of this submission. ASIC also works closely with other financial regulators on any ongoing cyber-related investigations.

ASIC's approach to engagement and capability building

23 ASIC takes a whole-of-Government approach to cyber supervision and incident response. We work closely with domestic and international government agencies to align priorities and coordinate consequence management, including through participation in:

(a) the Cyber and operational intelligence led exercices (CORIE) framework;

(b) the Ciminal Justice and Law Enforcement Forum on cybercrime;

(c) the CFR Cyber Security and Operational Reslience Working Group;

(d) the Cyber Security Regulators Network; and

(e) discussions with various domestic and international regulators and agencies as part of incident response or to progress joint cyber initiatives.

24 We engage regularly with industry bodies, CFR agencies, the Department of Home Affairs (DoHA), the Department of Treasury, the ASD, and the Office of the Australian Information Commissioner (OAIC). We are currently working closely with CFR agencies, Treasury and DoHA to implement the recommendations of the *2023-2030 Australian Cyber Security Strategy*.

25 We also proactively engage with industry and industry associations, such as the Australian Institute of Company Directors, Governance Institute of Australian and through the ASIC Cyber Consultative Panel.

Cyber and operational intelligence led exercices (CORIE)

26 The CFR developed the CORIE framework to assess entity's cyber resilience to advanced and persistent threats by simulating real-world attacks by cyber actors. The CORIE framework is enhanced by intelligence enrichment from the ASD's ACSC.

27 The CORIE team coordinators invite financial institutions and critical third parties to participate in the exercises in rounds, working closely with third-party cyber adversary simulators.

28 CORIE provides participating organisations with a framework to assess their cyber resilience by targeting their most critical business services. Participating in CORIE provides participants with valuable experience in managing incidents, identifying gaps in incident response plans and playbooks, and gaining a better understanding of the roles and responsibilities allocated within the teams. Participation enhances each organisation's ability to prevent, detect, and respond to significant threats.

Cyber pulse survey

29 ASIC developed the cyber pulse survey in 2023 to better understand the cyber maturity, threats, and challenges of regulated organisations in the ongoing heightened threat environment. The anonymous, voluntary survey was designed to help organisations assess their cyber resilience and allow them to benchmark their cyber maturity against their peers.

30 Ninety-five of participants elected to receive an individual report with insights on how they assessed their cyber resilience capability compared to similar organisations in their industry, demonstrating a commitment to improving their

cyber security. Individual feedback reports identified areas for improvement and suggested practices to improve organisational cyber capabilities.

31 The survey invited participation from approximately 40,000 public companies, large proprietary companies and entities that hold licences or authorisations from ASIC. The findings from the survey were published in Report 776 *Spotlight on cyber: Findings and insights from the cyber pulse survey 2023*. The report, which is designed to encourage uplift across Australia's corporate sector, outlines key findings from the survey, summarises important trends, identifies areas for improvement and highlights better practices with practical examples.

MoneySmart

32 ASIC has run digital campaigns and published information about online safety through its MoneySmart website. Consumer education has focused on identifying financial scams (including credit card and crypto scams), online shopping and identity theft.

33 Since July 2023, ASIC has disrupted scam activity by initiating takedowns of more than 2,500 investment scam and phishing websites. The new scam website takedown capability implemented by ASIC removes or limits access to fraudulent and malicious websites on the internet and expands on a three-week trial ASIC conducted in 2022.

Limitations of existing approaches

34 In the 12 months since the Optus cyber incident of September 2022, ASIC has been involved in four nationally-coordinated cyber consequence management activities.

35 ASIC has also been involved in, or led, an additional four CFR-coordinated incident responses. While some involved service disruption, all incidents stemmed from an exfiltration of data.

36 However, it is only a matter of time before business disruption, and not ransom for data, is the focus of one of these attacks. With rising geopolitical tensions, the incidence, severity and likelihood of such a cyber attack will only increase.

Case study

37 ASIC recently led the coordinated response to a cyber incident on a regulated entity. The incident was the result of an attack through a key third-party service provide. A service provider that is extensively engaged by organisations throughout Australia's financial services sector and beyond.

38 In the aftermath of the incident, the affected entity (and the government agencies with which the identity of the vendor was shared) were not permitted to voluntarily share the name of the impacted vendor with ASIC, even as a matter of urgency. At the time, ASIC had substantial concerns that the third-party service provider may pose a systemic risk to Australia's financial services sector.

39 While the risk was not realised in this instance, the delay in intelligence sharing could have increased the broader impact of the incident with widespread consequences for Australia's financial system. This incident highlighted the shortcomings in available mechanisms to support information sharing that enables appropriate consequence management by ASIC.

40 While compulsory powers may have resulted in the production of details about the third-party supplier in the case study, ASIC is concerned this approach is inefficient and inadequate – particularly if the affected organisation's systems are unavailable and their resources are being diverted to restoration and incident response.

Information sharing

41 The lessons learned from ASIC's involvement in the coordinated responses to these cyber incidents, has led ASIC, together with other CFR agencies, to engage with DoHA and ASD on sharing of:

(a) cyber threat intelligence, and

(b) details of cyber incidents impacting our regulated entities, or key suppliers of those entities.

42 Intelligence sharing at the initial stages of a cyber incident is vital to ensuring the integrity of Australia's financial markets by facilitating an efficient and timely response. Visibility of issues throughout the supply chain is essential to maintaining the stability of Australia's financial system given the interconnected nature and criticality of financial markets infrastructure and intermediaries.

43 Access to timely information would assist ASIC to mitigate the consequences and broader impact of a cyber incident on Australia's financial system and ensure it meets its regulatory functions of maintaining fair and efficient markets and minimising harm to consumers and investors. Efficient information sharing between agencies may also reduce the reporting burden on affected entities.

44 These conversations have been held bilaterally with relevant agencies and through appropriate working groups.

Limited use obligation

45 Timely information sharing between affected entities and regulators is essential to mitigating the systemic impact of a cyber incident. However, fear of regulatory action can deter organisations from sharing information with government.

46 In response to industry concerns around information sharing with regulators during and following a cyber incident, ASIC notes the 22 November release of Government's *2023-2030 Australian Cyber Security Strategy* which proposes the introduction of a legislated 'limited use' obligation preceded by an interim Statement of Comfort. The obligation is intended to provide clarity and assurance to industry around how information they share with the ASD and Cyber Coordinator can be used by other Australian Government entities, including regulators.

47 The obligation would prevent ASIC from using the information as part of any investigation or enforcement action. Importantly, enforcement action is not the reason we are seeking access to this information, our intention is to seek this intelligence to manage the broader impacts of a cyber incident on Australia's financial system.

48 The 'limited use' obligation does not affect industry's regulatory obligations, provide immunity from legal liability or limit ASIC's regulatory powers to compel information if needed. These are the avenues we would pursue for enforcement action.

49 Practically, this means that only technical circulars would be shared with all registered ACSC partners at the same time.

Can the limited use obligation be extended?

50 Over the last 12 months, ASIC has engaged with relevant Government agencies on the limitations of current information-sharing arrangements. Specifically, we have held bilateral discussions with the ASD around our interest in a high-level information-sharing arrangement where an incident involves an ASIC-regulated entity, or a key service provider to the financial services and markets sectors, and which may pose a systemic risk to Australia's financial markets and infrastructure.

51 ASIC is seeking this information to minimise harm and manage consequences of an incident. We are not seeking access to information to compile evidence for future enforcement action against an entity where they may have failed to adequately manage their cyber-related risks. Our intention to encourage information sharing by impacted entities without the risk of regulatory reprisal is

consistent with the whole-of-Government perspective, however, the mechanism is yet to be agreed.

52 We are supportive of Government's efforts to incentivise and improve reporting around cyber incidents. However, we do not see how the overarching purpose for seeking this protection (i.e. knowledge building for early intervention) is achieved by excluding regulatory authorities from access to information for consequence management purposes.

53 We urge the development of an effective and timely information-sharing mechanism that facilitates proactive intervention aimed at minimising the harm of a cyber incident on consumers and the broader financial system.

Key terms

Term	Meaning in this document
ASIC	Australian Securities and Investments Commission
ASIC Act	*Australian Securities and Investments Commission Act 2001*
Inquiry	Parliamentary Joint Committee on law enforcement inquiry into the capability of law enforcement to respond to cybercrime
PJC	Parliamentary Joint Committee on Law Enforcement