Cyber Risk

September 2022

Contact	Senior Executive Leader	Executive Director
s 22 [redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Key Messages

Working with other agencies, ASIC is partnering with industry to make Australian financial services and markets cyber vigilant.

ASIC's win in the RI Advice matter this year is the first of its kind in Australia, and clearly signals that Financial Services licensees must adequately manage cybersecurity risks as part of their licence obligations so as to protect consumers.

While we recognise it is impossible to reduce cybersecurity risk to zero, entities can take action to reduce that risk, and reduce the potential of harm to their consumers. All organisations should regularly re-assess their cyber risks and ensure their detection, mitigation and response measures adequately support the size and complexity of their business, and the sensitivity of the information they hold.

Background

The Australian Cyber Security Centre estimates that Cybercrime cost Australia $42b in 2021

In July 2022 the Australian Institute of Company Directors published their findings from 'The Boards and Cyber Resilience' study. This survey revealed that 72 per cent of directors that participated see cybersecurity as a ‘high priority’ issue for their board.

Collaboration with other agencies

ASIC is working in close collaboration with other financial regulators to:

- review, align and coordinate cyber supervision activities to achieve better outcomes for the financial sector through sharing of resources, skills and knowledge;
- execute joint projects and activities, e.g.:
- CFR and Trans-Tasman cyber incident response protocols
- Cyber Operational Resilience Intelligence-led Exercises (CORIE) project involving key financial firms; and
- provide input to Home Affairs on the proposed cyber regulation for critical infrastructure entities, particularly on thresholds for inclusion for Positive Security Obligations (PSO).

ASIC is also engaging in forums chaired by the Department of Home Affairs to support the Australian Government cyber agenda. The CFR Cyber Security Working Group has recently expanded to also include in discussions the ACCC, Home Affairs, Australian Communications and Media Authority and the Office of the Australian Information Commissioner. This group is working to provide:

- Clarity on various regulatory remits of the agencies outside of CFR
- Better understanding of information sharing barriers between agencies
- Stronger collaboration between agencies and
- Minimising inconsistent or misaligned government messaging, regulation and requirements.

In addition to partnering locally with agencies, we also engage with international financial regulatory authorities to learn from their experiences and discuss their approaches.

ASIC Action

Enforcement action - RI Advice
In May 2022, the Federal Court found that RI Advice Group Pty Ltd had a number of inadequate cyber risk management practices across its network which amounted to a breach of its license obligations to act efficiently and fairly. This included some of its authorised representatives failing to have up-to-date antivirus software, system backups, email filtering or quarantining, and poor password practices. Inadequacies in its cybersecurity risk management lead to a number of cyber incidents affecting clients in the six-year period to May 2020.

Following this decision ASIC articulated our expectations of AFS licensees including:

- entities should adopt good cybersecurity risk management practices to reduce potential harm to consumers. We expect active management of cyber risks and continuous cybersecurity improvement.
- AFS licensees need to act quickly in the event of a cyber incident to minimise the risk of ongoing harm. Theft of sensitive personal information can significantly affect consumers' financial and physical well-being and can be long-lasting.
- we strongly encourage AFS licensees to report cyber incidents to the ACSC. Licensees should also consider if any obligation arises to report the incident to ASIC.

Industry engagement - ASIC Cyber Consultative Panel
ASIC has formed a cyber consultative panel, with the first meeting held in May 2022. The role of the Panel is to provide ASIC strategic advice from an industry perspective on:

- best practices in cyber and operational resilience and related fields
- emerging cyber and operational resilience trends, risks and issues
- any significant obstacles and barriers for the delivery of ASIC's cyber and operational resilience strategy.

ASIC review of cyber resilience of markets firms
Key findings of ASIC Report 716 Cyber resilience of firms in Australia's financial markets: 2020-21 (published Dec 2021)

- there has been a small, but steady, improvement in the cyber resilience of firms operating in Australia's financial markets, however the increase of 1.4% falls far short of the 14.9% improvement targeted for the period
- the gap between large firms and small-to-medium enterprises (SMEs) is continuing to close
- the cyber resilience of many SMEs has improved
- the confidence of larger firms in their own cyber resilience has fallen slightly
- the level of cyber resilience for supply chain risks has remained relatively static since ASIC last conducted the self assessment in 2018-19.