APRA and ASIC host Superannuation CEO Roundtable

9 June 2023

APRA and ASIC held a Superannuation CEO Roundtable on Monday, 29 May 2023. The focus of the discussion was Cyber Resilience. Hosted by Margaret Cole, Deputy Chair, APRA, and Danielle Press, Commissioner, ASIC, the Roundtable was attended by fourteen superannuation trustee Chief Executive Officers (**CEOs**) and other executives, representing a broad cross-section of the industry. Shane Moore, Director, Superannuation and Employer Obligations from the Australian Taxation Office also attended the Roundtable (see **Appendix II** for the full list of attendees).

Cyber Resilience

In our growing digital economy, the frequency, breadth and scale of cyber-attacks is escalating rapidly. As a result of growing scam, fraud and cyber threats, it is crucial that all superannuation trustees have adequate measures in place now to prevent, detect and respond to these threats.

APRA and ASIC provided an overview of Government and regulatory initiatives of relevance, with a focus on cyber threats (see **Appendix I**). The importance of early regulatory engagement in the event of a cyber-attack was emphasised and it was noted that, depending on the nature and scale of the incident, a whole-of-government response could be triggered.

Insights from lessons learnt from recent cyber-attacks in Australia, both within and outside of the superannuation industry, were shared by the regulators and included the following:

- To reduce the risk of significant compromise, trustees should have strong data and IT systems governance measures that include the decommissioning of legacy systems and adequate service provider oversight.
- Preparedness for an incident occurring is also critical. Response plans should be tested and address, at a minimum, governance and decision-making, business continuity and contingency planning, and communication strategies.
- Simulations of cyber threats and trustee responses can be very effective in ensuring that trustees are well-prepared and response plans are fit for purpose. Clear delineation between board and management responsibilities is important to establish in advance of any real threat scenario.
- Cyber incidents can have direct negative consequences for members. Trustees must make decisions which are in the best interests of their members and this includes providing members with timely and accurate communications and ensuring adequate resourcing for appropriate member support.

The CEOs expressed an interest in sharing information relevant to addressing cyber risks more regularly and rapidly within the industry. The CEOs acknowledged the importance of protecting data held by the trustee and its service providers and the need to ensure effective controls were in place across the supply chain.

The CEOs shared practices on how their organisations have uplifted cyber resilience, such as by reviewing their data management plans and implementing changes, uplifting the cyber capability of the Board and key internal stakeholders, and developing and testing the operating effectiveness of response plans to material cyber incidents. The CEOs also acknowledged the importance of protecting the growing volume of data held, particularly in relation to personal information.

APRA and ASIC urged industry participants to consider establishing, as soon as practicable, a cross-industry forum to discuss trends and share learnings in relation to cyber risks and incidents. While privacy, commercial and competition considerations are important, the CEOs agreed that a 'safe space' to share experiences would be of great benefit. APRA and ASIC are willing to play an appropriate role to encourage such discussions.

APRA and ASIC highlighted that they plan to host more frequent CEO Roundtable events in the future and closed the meeting by noting that they will continue to engage with each other, the industry and other regulators, about cybersecurity best practices.

Appendix I – Recent and Upcoming Government and Regulatory Initiatives

Australian Prudential Regulation Authority

- APRA's Prudential Standard CPS 230 Operational Risk Management is designed to strengthen the management of operational risk in the banking, insurance and superannuation industries. An updated standard commences on 1 July 2025.
- APRA's Prudential Standard CPS 234 Information Security (**CPS 234**) aims to ensure that APRA regulated entities take measures to be resilient against information security incidents. APRA's CPS 234 Tripartite Review program requires selected entities to have an independent assurance practitioner review their compliance against CPS 234.
- APRA letter to all APRA regulated entities dated 26 May 2023 titled Use of multi-factor authentication notes that multi-factor authentication (**MFA**) has not been adopted as a standard practice across the industry and outlines APRA's expectation that trustees and other APRA-regulated entities review the coverage of MFA in their operating and technology environments.

Australian Securities and Investments Commission

- In April 2023, ASIC called for all financial institutions to improve their approaches to handling scams following a review of bank practices (see ASIC Report 761: Scam prevention, detection and response by the four major banks).
- In June 2023, ASIC will launch its Cyber Pulse Survey. The survey has been designed to help financial service entities better understand their cyber resilience capability.

Other

- In July 2022 the Council of Financial Regulators released an updated version of the Cyber Operational Resilience Intelligence-led Exercises framework (**CORIE**). The framework has been designed to test and demonstrate the cyber maturity and resilience of institutions within the Australian financial services industry.
- The Privacy Act 1988 regulates the collection, use, storage and disclosure of personal information by relevant entities. A review of the Privacy Act 1988 has been undertaken with a view to strengthening requirements on entities to keep personal information secure and destroy or de-identify it when it is no longer needed.
- Security of Critical Infrastructure Act 2018 provides for mandatory cyber incident reporting for critical infrastructure assets, which includes superannuation funds.

- Australian Government Crisis Management Framework outlines the Australian Government's approach to preparing for, responding to and recovering from crises. This can include large scale or complex cyber incidents.
- In December 2022, the Government appointed an Expert Advisory Board to advise on the development of the 2023-2030 Australian Cyber Security Strategy.
- The ATO convened Superannuation Industry Stewardship Group established a working group in November 2022, led by APRA, to understand and document fraud risks, and the effectiveness of existing controls, including actions required to strengthen/mitigate against emerging risk areas to safeguard member accounts and member data.

Appendix II – CEO Roundtable attendees

Superannuation Executives	
Bernard Reilly	Chief Executive Officer, Australian Retirement Trust Pty Ltd
Deanne Stewart	Chief Executive Officer, Aware Super Pty Ltd
Debby Blakey	Chief Executive Officer, H.E.S.T. Australia Ltd
Jason Murray	Chief Executive Officer, Motor Trades Association of Australia Superannuation Fund Pty Limited
Kate Farrar	Chief Executive Officer, LGIAsuper Trustee
Kelly Power	Chief Executive Officer, Avanteos Investments Limited
Kristian Fok	Acting Chief Executive Officer, United Super Pty Ltd
Paul Cassidy	Chief Executive Officer, Guild Trustee Services Pty Limited
Paul Schroder	Chief Executive Officer, AustralianSuper Pty Ltd
Peter Chun	Chief Executive Officer, Unisuper Limited
Renato Mota	Chief Executive Officer, Insignia Financial Ltd
Ruby Yadav	Chief Executive Officer, Superannuation Services, Mercer Australia
Scott Cameron	Chief Executive Officer, Togethr Trustees Pty Ltd
Vicki Doyle	Chief Executive Officer, Retail Employees Superannuation Pty Limited

APRA attendees	
Margaret Cole	Deputy Chair
Carmen Beverley Smith	Executive Director, Superannuation
Clare Gibney	Executive Director, Policy and Advice
Adrian Rees	General Manager, Superannuation
Mike Cornwell	General Manager, Superannuation
Katrina Ellis	General Manager, Superannuation
Lucinda McCann	General Counsel, Legal
Alison Bliss	General Manager, Operational Resilience
John Singh	Head of Operational Resilience Transformation

ASIC attendees	
Danielle Press	Commissioner
Jane Eccleston	Senior Executive Leader, Superannuation
Amanda Zeller	Senior Manager, Regulatory Cyber and Operational Resilience Centre

Sacha Vidler	Senior Manager, Superannuation

ATO attendee	
Shane Moore	Director, Superannuation and Employer Obligations

Signed

Margaret Cole
Deputy Chair
Australian Prudential Regulation Authority
www.apra.gov.au

Danielle Press
Commissioner
Australian Securities and Investments Commission
www.asic.gov.au