Securing the future

Protecting Australia's superannuation ecosystem against cybersecurity threats

pwc

Gateway Network Governance Body

Table of contents

The risks we face

What are the most common cyber incidents across the superannuation ecosystem?

75%

Theft of member data
Stolen member data used to commit fraud

72%

Third party compromise
Unauthorised access resulting from 3rd party / related party being compromised

71%

Privacy Breach
Loss of personally identifiable information resulting in privacy breach

64%

Systems disruption
Cyber incident causing inability to perform critical functions such as service members or manage investments

Percentage of survey respondents who advised these incidents occur often and sometimes.

> ***"Super is an attractive target – compared to bank accounts, day to day engagement is lower and the pace of digitisation has vastly increased the attack surface"***
>
> *Industry representative*

Common threats

What are the most common cyber threats across the superannuation ecosystem?

82% **Phishing emails**

56% **Identity theft / impersonation**

55% **Human error / negligence**

46% **Malware (computer viruses, etc.)**

Percentage of survey respondents who advised these threats occur often.

> ***"Phishing is still out biggest attack – looking for staff and member credentials"***
>
> *Retail Super Fund Representative*

The Superannuation ecosystem

A unique, sizeable and highly networked environment

$3 trillion
in assets

165 million
transactions per year processed by Gateway Operators

24.4 million
member accounts

+880k
Employers

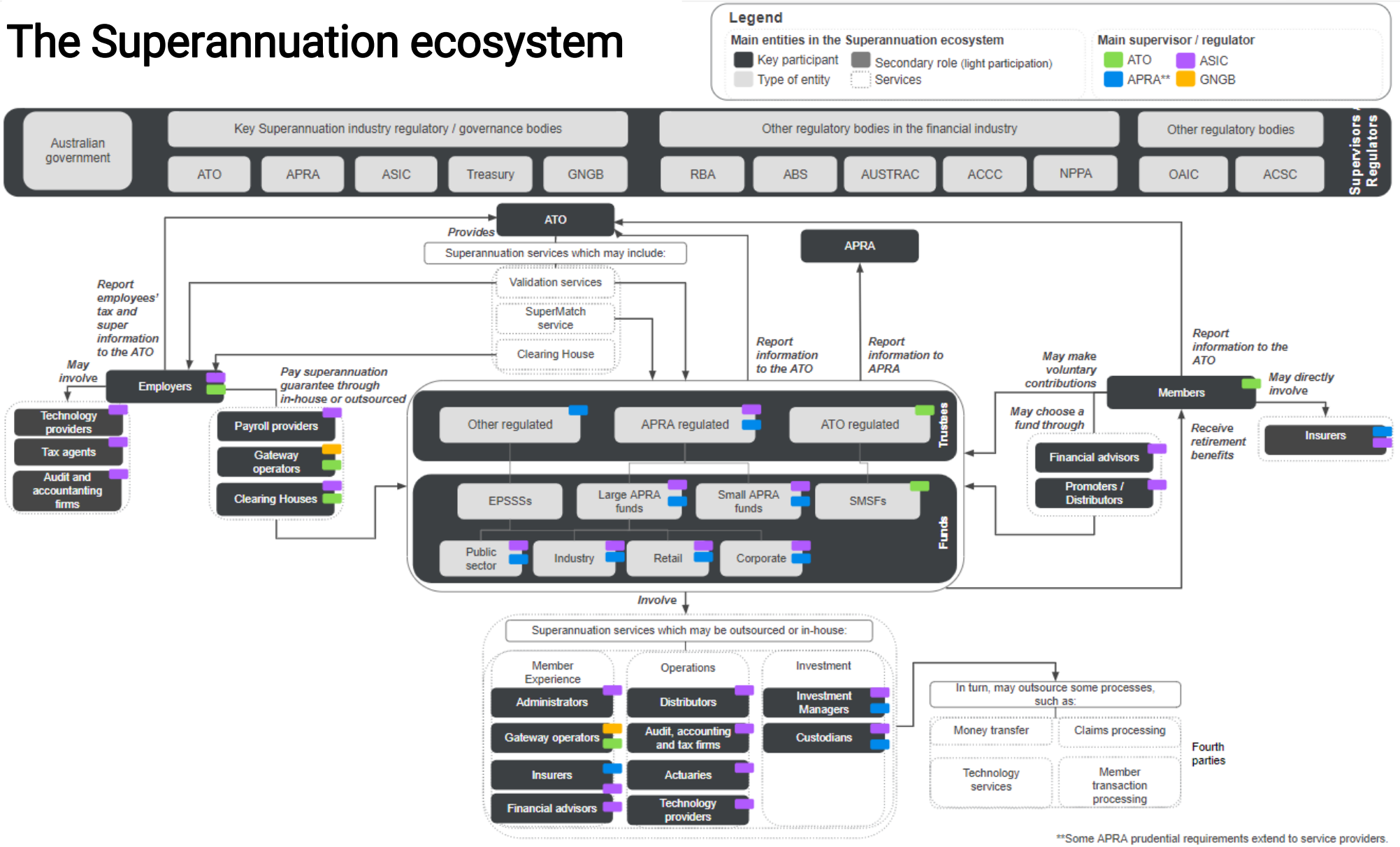
+593k
SMSF's

+300
payroll providers

101 *retail funds*
35 *industry funds*
25 *Pooled super trusts*
19 *public sector*
17 *Corporate funds*

9 *Gateways*
11 *custodians*
2 *administrators*

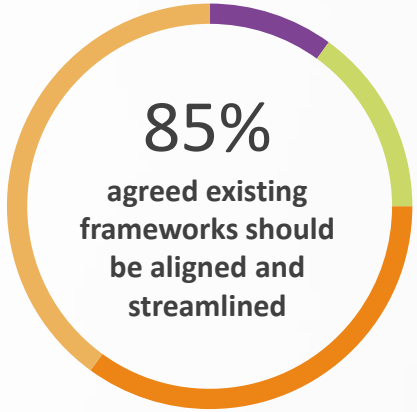
The Superannuation ecosystem



A fragmented yet evolving regulatory landscape

Regulatory challenges

- Australian **regulation of the superannuation ecosystem in relation to cyber is still evolving**, with considerable room for improvement in areas such as clarifying roles, reducing overlap of responsibilities and reflecting current priorities.
- There are **siloed and inconsistent cyber-regulatory expectations** of entities across the superannuation ecosystem.
- In addition, even where standards exist for regulated entities, these are often principles based, leading to **inconsistent interpretation and application across organisations**.
- There is work to do to drive effective **end-to-end cyber resilience** and to adopt a **consistent sustainable approach** for all players in the ecosystem.
- A large number of small- to medium-sized organisations, such as employers or those providing services to employers, are **not required to meet cybersecurity standards** and/or may lack the guidance specific to their role in the ecosystem.



Facing the challenges

- There is a **lack of accountability and cyber risk leadership for end-to-end cyber resilience** of the ecosystem;
- There is **no common standard for cybersecurity**, and as a result approaches to managing cyber risks across the ecosystem are **inconsistent and uncoordinated**. It's worth noting that some ecosystem participants are global organisations with headquarters outside of Australia, creating a **global consistency challenge**;
- Compounding these challenges, there is **lower cybersecurity awareness among superannuation members** who, understandably, may not interact often with their superannuation; and
- Given the **barriers to sharing cyber threat intelligence** across the ecosystem and an absence of a trusted mechanism for doing so, it is difficult to systemically share instances of organisations or members being compromised.

Calls to actions

An industry, organisational and member approach to managing cyber risks

Challenge 1: Accountability and risk leadership

Clarify roles and responsibilities to build cyber resilience

Industry leaders

- Define a **framework** - clarify cybersecurity **roles and responsibilities**.
- Define a **consistent and practical approach** to address **third party security risks**.

Organisational leaders

- Drive a **cyber risk–aware culture** - **maintain a secure environment**.
- Maintain **secure products and services**

Members/individuals

- **Members to take accountability for their own data security** and practice secure online behaviours

Challenge 2: Inconsistent cybersecurity capabilities

The ecosystem needs to get the basics right

Industry leaders

- Define a **minimum and common baseline of cybersecurity controls** ecosystem-wide; practical for organisations of different size and complexity to implement.

Organisational leaders

- **Place cybersecurity at the forefront of business strategy**.
- **Monitor the effectiveness of baseline controls, including your third parties**.

Members/individuals

- Members to ask service providers how they are protecting your data and consider cybersecurity risks when selecting your service provider

Calls to actions (cont'd)

An industry, organisational and member approach to managing cyber risks

Challenge 3: Low levels of cyber awareness

Influence members' cyber awareness, education and practices

Industry leaders

- Collaborate on **cyber awareness campaigns and cyber education plans** for all individuals in the ecosystem including members.

Organisational leaders

- Implement **strong authentication techniques**, such as multi-factor authentication.
- **Prompt members to enable strong security settings** through their online portal or application features.
- **Communicate to members of the potential cyber risks and threats** through different distribution channels.

Members/individuals

- Members to know where to go to: **report suspicious events, understand how to protect their data**.

Challenge 4: Barriers to sharing threat intelligence

Put in place a structured, safe and confidential threat-sharing platform

Industry leaders

- **Examine barriers to sharing threat information**.
- Leverage existing initiatives to **create a formal, confidential forum to enable threat sharing** among a trusted group, led by an independent entity and with clear rules of engagement.
- **Co-develop and participate in cyber-detection strategies** that ecosystem participants can use (e.g. red teams, attack simulations).

Organisational leaders

- Leverage or expand on existing **resources to analyse and monitor threat information**.
- **Develop threat models** for defence and recovery strategies.

Members/individuals

- **Members to monitor accounts more frequently** and **report suspicious events** or potential threats (e.g. phone/sms scams, phishing emails).

Calls to actions (cont'd)

An industry, organisational and member approach to managing cyber risks

Challenge 5: The lack of a holistic cyber resilience strategy

Co-develop cyber response and recovery strategies

Industry leaders

- Define a dedicated superannuation cyber-governance body to help **coordinate response and recovery testing** from incidents affecting multiple organisations across the value chain.

Organisational leaders

- Continuously **improve cybersecurity capabilities in response to lessons learned** and changes in the threat environment.

Members/individuals

- Members to know where to go to **remain up to date with the most common online security risks**.

Questions and feedback

For more information about the research in this report, or to talk to us about working together to protect the superannuation ecosystem, contact us.

Gateway
Network
Governance
Body

Level 26, 44 Market St Sydney NSW 2000

www.gngb.com.au

One International Towers, Watermans Quay, Barangaroo NSW 2000

https://www.pwc.com.au/important-problems/cyber-security-digital-trust.html