Securing the future:

Protecting Australia's superannuation ecosystem against cybersecurity threats

Gateway
Network
Governance
Body

Contents

Disclaimer

This report has been commissioned by Gateway Network Governance Body Ltd ("GNGB"), and co-authored by PwC Australia and GNGB.

This report is not intended to be relied upon by anyone other than GNGB. The report was prepared solely for GNGB's use and benefit in accordance with and for the purpose set out in the PwC engagement letter with GNGB dated 8 October 2020. In doing so, PwC acted exclusively for GNGB and considered no-one else's interests.

PwC accepts no responsibility, duty or liability:

- To anyone other than GNGB in connection with this report; and
- To GNGB for the consequences of using or relying on it for a purpose other than that referred to above.

PwC makes no representation concerning the appropriateness of this report for anyone other than GNGB. If anyone other than GNGB chooses to use or rely on it they do so at their own risk.

This disclaimer applies:

- To the maximum extent permitted by law and, without limitation, to liability arising in negligence or under statute; and
- Even if PwC consents to anyone other than GNGB receiving or using this report.

PwC's liability is limited by a scheme approved under Professional Standards legislation.

Glossary of key terms

Superannuation ecosystem: Interconnected network of organisations that govern, participate and provide services across the superannuation system. The superannuation ecosystem spans some of Australia's largest financial institutions, over 880,000 employer organisations and the accountants, bookkeepers, clearing houses, gateways, administrators and more that comprise the supply chain.

Cybersecurity resilience: The ability to safeguard an account holder's member data, and withstand or quickly recover from cyber incidents in an attempt to protect superannuation savings.

Cyber risk: The potential likelihood and impact of loss events during which digital assets and services are intentionally or accidentally compromised.

Cyber threats: A threat actor's successful or unsuccessful attempt to compromise a digital asset or service.

Phishing: A targeted email or series of emails sent by a cybercriminal in an attempt to trick recipients into sharing sensitive information such as online banking logins, credit card details, business login credentials or passwords.

Ransomware: A type of malicious software or malware used by cybercriminals to restrict a recipient's access to files or services, often until payment is made.

Identity theft: A cybercriminals' efforts to access personal information to steal money, apply for loans or gain other benefits. Identity theft can involve the creation of fake identity documents using a victims' details along with a false photograph.

About this research

Among the myriad of negative headlines in Australia's news landscape over 2020, cyber threats loomed large. Cyber incidents, including ransomware infections and data breaches, were consistently reported across a wide variety of sectors, including transport, health and education. In response to increasing threats, in June 2020 the Prime Minister, Scott Morrison, issued a media release alerting all Australians of an active campaign of targeted attacks on a national scale[1]. Overall in 2020, cyber crimes directly affected almost one in three Australians and cost Australian businesses around $29 billion[2].

Comparatively, in Australia's superannuation industry, no material cyber incidents have been reported to date. While we have seen cases of stolen credentials used to fraudulently transact and access savings, a material systemic compromise in the superannuation ecosystem has not yet been identified. But we cannot afford to be complacent. The cyber landscape is changing: digitisation and remote working have accelerated as a result of the COVID-19 pandemic, and the changes we are seeing are here to stay.

Our superannuation ecosystem is used to change and deals with it well, but this new and growing threat calls on us to work together more closely than ever before.

Because of the interconnected nature of our superannuation ecosystem, we depend on each other to protect the superannuation savings of all Australians. The super ecosystem is complex, relying on a range of stakeholders including members, employers, advisers, payroll providers, gateway providers, administrators, custodians, investment managers, regulators and super funds to all work together to deliver the member experience. Given the rapidly evolving cyber landscape, we must all work together now to ensure that our services continue to safeguard the superannuation savings entrusted to us by retired and working Australians.

The Gateway Network Governance Body (GNGB) remit is to ensure the security, integrity and efficiency of the Superannuation Transaction Network (STN): the data infrastructure that transports contributions and rollover transactions. The STN relies heavily on the ability to identify and mitigate cyber risk. Given the interconnectedness of our superannuation sector, we set out to understand the following: What are the top cyber risks in the superannuation ecosystem? What are the most common cyber threats that introduce these risks? What are the main challenges for the ecosystem in managing these cyber risks, for both individual entities and as a collective? What actions should we take as an industry to improve cyber resilience in the ecosystem?

To help answer those questions, GNGB with PwC Australia, undertook a national research study and gathered the views of more than 80 executives and professionals across the superannuation industry. We offer sincere thanks to those individuals for sharing their experiences with us. This report captures these expert's insights and outlines practical strategies that we, as an industry, should consider for the long-term security of the superannuation ecosystem.

Though the results showed us that the journey to a cohesive approach will not be without challenge, it also showed us that we are as an industry a 'collective of the willing', and we now have a great opportunity. There is no better time to focus on our approach to cyber risks and to optimise our cyber resilience. We hope that you will join us – to debate, design and develop our path forward together.

Kind regards,

Michelle Bower
Executive Officer, GNGB

Executive summary

No industry is immune from cybersecurity attacks

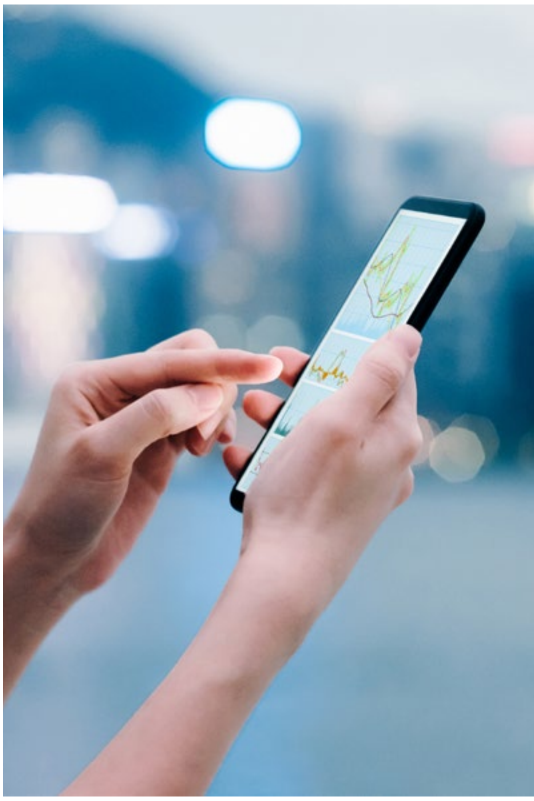
Superannuation is a crucial platform for the retirement and financial wellbeing of both working and retired people in Australia. But the superannuation industry and its supporting ecosystem, which processes assets of value, such as personally identifiable information for millions of members and manages approximately $2.9 trillion in funds[3], is a lucrative target for cybersecurity-related activity. In 2020 alone, the industry saw a number of cybersecurity-related attacks (and near misses) which have made the building of cyber resilience and trust within the ecosystem top priorities.

The key cybersecurity risks and incidents identified in this research include:

- Theft of member data that is then used to commit fraud for financial gain;
- Loss/theft of member data resulting in a privacy breach and associated fines and penalties; and
- Compromised business systems that affect business operations and therefore jeopardise member services and funds under management.

These risks are not unique to the superannuation industry, but the nature of its assets is such that failure to address them will result in far-reaching consequences.

It is crucial that we understand this industry's risks and challenges, and implement a coordinated capability to improve protection and cyber resilience of its ecosystem.



The secured future

With the input, effort and ownership of all stakeholders that comprise the superannuation ecosystem, imagine an ecosystem with the following cyber resilience characteristics as a possibility.

Characteristics	Benefits
All stakeholders in the ecosystem have consistently implemented and are appropriately managing the minimum essential cybersecurity controls.	This would lift the ecosystem's overall ability to protect itself from common and rudimentary cybersecurity attacks, which would in turn reduce the likelihood of a cyber incident.
A systematic process for sharing cyber threat and incident intelligence dynamically across the ecosystem.	As soon as a part of the ecosystem comes under attack, the rest of the ecosystem is made aware and appropriate responses and prevention plans can be put in place to minimise the risk of a repeat or ecosystem-wide disruption.
The capabilities to prevent or counter risks from member behaviour (accidental or intentional) are built into the ecosystem rather than being solely the responsibility of members.	Members are alleviated from being solely responsible for maintaining a high level of security.
A well-rehearsed and coordinated ecosystem-wide approach exists for responding to cyber incidents, including continual testing and improvement.	Organisations are prepared to rapidly and effectively respond to cyber incidents, minimising potential impacts to themselves as well as their ecosystem.

In the above imagined future, common cybersecurity attacks would be prevented and damage from more choreographed or advanced attacks blunted.

The importance of a coordinated approach

Facing the challenges

To realise an ecosystem with such cyber characteristics, this research identified that the following challenges need to be addressed:

- There is a lack of accountability and cyber risk leadership for end-to-end cyber resilience of the ecosystem. While there are a number of regulators in the ecosystem, each has a different area of focus and none has ultimate or overall accountability;
- There is no common standard for cybersecurity, and as a result approaches to managing cyber risks across the ecosystem are inconsistent and uncoordinated. Not all stakeholders in the ecosystem are required to adhere to a standard (e.g. the Australian Taxation Office (ATO)'s Digital Service Providers (DSP) Operational Framework or the Australian Prudential Regulation Authority (APRA)'s Information Security Cross-Industry Prudential Standard CPS 234), and among those organisations that do adhere to one, those standards are not always applied with the same level of consistency and maturity. 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.

In combination with the lack of a holistic and coordinated approach to respond to cyber incidents in the ecosystem, it is only a matter of time before a well-coordinated cyber attack could result in significant and widespread disruption.

Building sustainable cyber resilience

The time is now

The time to address these challenges is now. The post COVID-19 pandemic acceleration of digital initiatives in 2020, coupled with the increased options for members to interact with, and access their superannuation early, has also multiplied the nature and range of cybersecurity risks for the industry. We need to come together and collectively take responsibility in order to move forward.

The superannuation ecosystem needs an overarching strategy to combat cyber risk, which includes the following elements:

- Roles and responsibilities for building cyber resilience in the ecosystem need to be clarified;
- A basic set of standards (e.g. the Australian Cyber Security Centre (ACSC)'s Essential Eight and underpinning controls) need to be agreed upon and consistently implemented across all parts of the ecosystem. This also includes addressing legacy systems;
- A coordinated system-wide approach is needed to influence and educate member awareness and behaviour in relation to cybersecurity risks;
- A structured, safe and confidential cyber threat-sharing platform for all ecosystem participants needs to be designed and implemented; and
- A coordinated cyber response and recovery strategy needs to be developed and regularly tested.

Embracing cyber resilience may seem daunting at first, but minor actions can make major change when it comes to building a robust retirement savings system for all Australians. As an industry, we should consider the following first steps:

1. Holding a roundtable of key representatives of all entities in the ecosystem to establish a working group; and
2. Establishing the working group's terms of reference and a specific timeframe for the working group to achieve a desired and agreed outcome: an ecosystem-wide strategy and plan for cyber resilience.

Ultimately, the continual protection of members' privacy and financial wellbeing will not happen automatically. It is up to all ecosystem participants to come to terms with the systemic risks that cyber poses. We must come together to coordinate a sustainable cyber resilience strategy that ensures our superannuation ecosystem can continue to support a quality of life that both working and retired individuals in Australia deserve.

The superannuation ecosystem: A highly attractive target for cybercriminals

Sensitive member data, retirement savings and reputations are all at risk in the event of a cyber attack. It is critical to identify cyber risk events, their potential impacts and how these risks can arise in the superannuation ecosystem.

What is at risk?

Cyber resilience in the superannuation ecosystem primarily involves the protection of member data, sensitive corporate and financial data (such as investment information), and ultimately the safeguarding of members' superannuation savings. With over 24.4 million superannuation accounts and approximately $2.9 trillion in assets, the Australian superannuation system is one of the largest in the world[4]. Working and retired people in Australia are dependent on the superannuation ecosystem for their wellbeing, long-term financial stability and quality of life in their retirement years.

An evolving superannuation ecosystem and digital threat landscape introduce risks that could result in the loss of members' superannuation savings and disruption of the digital ecosystem infrastructure, potentially leading to loss of trust in the Australian superannuation ecosystem.

Cyber threats pose a system-wide risk, and could represent significant threats for superannuation members, fund managers and the entire ecosystem itself. Their risk cannot be overstated.

What are the potential impacts of cyber risks on the superannuation ecosystem?

The impacts of cyber incidents across the superannuation ecosystem are potentially significant, as outlined below.

1. Loss of member superannuation savings

Stolen member data that is used to commit fraud, was identified by survey respondents as the most common cyber incident. Cybercriminals, motivated by financial gain, leverage stolen member data or user credentials to obtain unauthorised access to online superannuation accounts. These incidents could lead to fraudulent withdrawals or transfers of members' retirement savings into forged bank accounts. As customer identification procedures are not generally performed for incoming transactions, the risk of fraudulent or suspicious activity not being detected in a timely manner is elevated.

This threat is real: recent APRA data shows that by the end of October 2020, regulated superannuation funds had reported a total of 1,703 fraudulent payments – out of a total of 4.5 million Early Release Scheme payments – to members[5]. While this remains a relatively small percentage of total withdrawals (0.04%), it illustrates that the increasingly digitised nature of super transactions are increasing cyber risks. Furthermore, these

> **"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

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

75%
Stolen member data used to commit fraud.

72%
Cyber incidents resulting from a third party/related party being compromised.

71%
Loss/theft of personally identifiable information, resulting in a privacy breach.

64%
System disruptions that affect business operations.

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

reported incidents represent only detected incidents among regulated entities. Given the generally low levels of member engagement with their super, it may take some time before other cyber incidents are identified. As this data does not cover non-regulated organisations in the ecosystem nor non-reported incidents, the actual number of fraudulent incidents of this nature could be higher.

Other types of incidents such as targeted attacks at accounts payable via impersonation have also occurred within the superannuation ecosystem, however these are not specific to the industry.

Organisations are also increasingly facing regulatory consequences of cyber incidents. In August 2020, the Australian Securities and Investments Commission (ASIC) filed the first-of-its-kind legal proceedings against RI Advice, an Australian financial services licensee, for failing to have adequate cybersecurity systems in place. From 1st of January 2022, Section 56 of the Financial Sector Reform (Hayne Royal Commission Response) Bill 2020 concerning the extension of indemnification prohibitions will also mean that any future civil or criminal penalties can no longer be funded from member funds, creating another area of exposure for Trustees.

Further, organisations that suffer a security breach of their member data may be fined under the Privacy Act 1988 (Privacy Act) or legally required to pay compensation to individuals whose personal data was compromised. In 2020, the Australian Government announced an intention to amend the Privacy Act: the maximum penalties payable by organisations with a data security breach would be increased to the higher of either $10 million – three times the value of any benefit obtained through misuse of information or 10% of the organisation's annual domestic turnover.

Fines may limit capital for investment and could ultimately impact member experience, member returns and brand reputation.

2. Crippled service capabilities caused by disruption of digital ecosystem infrastructure

As the ecosystem is highly networked and dependent on third (and subsequent) parties, disruptions in its digital infrastructure could affect multiple organisations across the ecosystem. The time in which to respond and the capacity to quickly contain a multi-party cyber incident may be further delayed by the lack of an industry-wide incident response plan. Considerable time may lapse before business operations and services across the supply chain are fully restored.

An outage of key networks or IT systems could disrupt critical business operations and services to members. These incidents could temporarily cripple trading and investment capabilities of investment managers, potentially resulting in lower annual member returns. Such cyber incidents could also prevent members from accessing their online accounts, changing investment options, making additional contributions, initiating rollovers or withdrawals. When these transactions are temporarily unavailable, members may miss out on market opportunities and experience delayed income streams, with negative impacts on their overall returns and erosion of trust in the system.

In 2020, an example of this type of cyber incident included the multi-day outage experienced by the New Zealand Exchange (NZX). NZX websites were impacted for several days due to a Distributed Denial of Service (DDoS) attack - an attempt to render an online service unavailable by overwhelming it with internet traffic. Trading was maintained after switching to a contingency plan, however this example shows the impact of third party incidents in an organisation, as this attack originated from offshore via NZX's network service provider[6].

87%

of respondents agreed that the industry should colaborate to co-develop response strategies for incidents that affect multiple entities.

Our research found a current lack of response strategies or plans to recover from cyber incidents that affect multiple organisations across the ecosystem supply chain – a serious risk to the ongoing operation and viability of the ecosystem. Moreover, 87% of survey respondents indicated that organisations should collaborate more to develop response strategies for cyber incidents that potentially affect multiple organisations in the ecosystem.

In addition to the risks identified above, there is the possibility of a cyber attack that involves the theft of a large amount of funds under management. While research participants acknowledged this could significantly impact the ecosystem, it was not deemed to be a very likely event. Further, incidents of this nature have required fraud or business process control failures in addition to cyber activity, and as a result are not a focus of this report.

3. Erosion of trust in the Australian superannuation system

Cyber incidents can have significant operational, financial and reputational impacts on not only businesses and members, but also the Australian superannuation system itself.

- If member trust in the system erodes and they feel unable or unwilling to rely on trustees and the other parties to protect their retirement savings and data, they may decide to stop additional contributions and rely on other investment instruments. This behaviour would eventually undermine industry growth. Members may decide to switch to a self-managed superannuation fund (SMSF) as they perceive they may have more control over their fund and data;
- Members may decide to stop using additional services in the superannuation ecosystem, such as insurance products and financial advice, in fear that their information is not well protected. Again, such behaviour could thwart growth prospects in the superannuation industry;
- Businesses across the ecosystem may find it harder to trust third parties to securely process and protect member data on their behalf. This would make it harder for these organisations to find trustworthy service providers, which could impact their operations, and ultimately member experience; and
- Government may lose confidence in the superannuation industry's ability to deliver what it was originally tasked to do – protect and grow the retirement savings of workers in Australia. That could impact policy settings and, in the longer term, the operating model of the superannuation ecosystem.

To date, Australia's superannuation ecosystem has not reported a major, sector-wide incident. However, it has become increasingly clear that cyber risks pose system-wide risks which could lead to devastating impacts for the super ecosystem. The Australian Government also recognises this in its Security Legislation Amendment (Critical Infrastructure) Bill 2020, which seeks to expand the range of critical infrastructure entities that are protected to, among others, financial services and markets, data storage or processing entities, and health care and medical entities. As the number of cyber threats and incidents increase, now is the time to act and build a cyber resilient superannuation ecosystem.

How are cyber risks introduced into the superannuation ecosystem?

A variety of cyber threats for the super ecosystem can lead to the cyber incidents discussed earlier. Our research identified that phishing emails, identity theft, human error and malware (e.g. ransomware) are among the most commonly noted threats in the ecosystem. Some of these threats are on the rise and becoming more sophisticated. The ACSC reported that in the last year, ransomware incidents had significantly increased and are expected to continue increasing[7]. Phishing emails are becoming increasingly sophisticated and convincing, replicating messages from reputable senders and targeting individuals with access to highly sensitive personal or financial data.

Cybercriminals exploit vulnerabilities, such as weak access controls, unpatched software and open ports, to not only access systems holding sensitive data but also gain unauthorised access to member accounts, allowing them to make fraudulent rollover or withdrawal requests. According to the ACSC, many of the techniques used by cybercriminals to compromise sensitive personal and financial data can be mitigated through simple measures, such as not responding to unsolicited emails and text messages, and implementing stronger authentication mechanisms (e.g. multi-factor authentication)[8].

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, ransomware, etc.)

Percentage of survey respondents who advised these threats occur often.

> **"Phishing is still our biggest attack – looking for staff and member credentials."**
>
> Retail super fund representative

An increasingly targeted ecosystem

Why is the superannuation ecosystem increasingly targeted?

- **The size of the industry's membership and assets make it an attractive target:** The main assets targeted are confidential member data, with the ultimate aim of stealing members' retirement savings. With 24.4 million superannuation accounts and $2.9 trillion in assets (one of the largest in the world)[9], the Australian superannuation ecosystem is a highly attractive environment for cybercriminals. In addition, increasing digitisation and interconnectivity of services expand the ecosystem's cyber threat environment;
- **Superannuation members are historically less likely to monitor their superannuation accounts** compared to, for example, a transactional banking account. This decreases member likelihood of identifying and reporting unusual account activity. More than half (54%) of survey respondents indicated that members' infrequent checking of their accounts is one of the main drivers of cyber risk in superannuation. Malicious actors prefer to target environments in which their actions are less likely to attract notice; and
- **Cybercriminals are becoming increasingly sophisticated.** The primary motivation of cyber threat actors is to steal individuals' personal and financial information with the aim of generating profit[10]. These actors are becoming increasingly sophisticated. Hacking tools, playbooks and cybercrime-as-service products are becoming readily available through underground black markets (often referred to as darknet marketplaces). As a result, illicit tools, services and stolen data are accessible and, in many cases, minimal technical expertise is needed to launch cyber attacks.

In addition to the above factors, the unique characteristics of the superannuation ecosystem also add a layer of challenges for effectively managing cybersecurity risk – we examine these challenges next.

A unique, sizeable, dynamic and highly networked ecosystem

The Australian superannuation ecosystem is one of a kind, highly networked and dynamic. It continues to evolve as it matures and regulation changes. Understanding its intricacies is a critical starting point for building cyber resilience.

Unique

The 2020 Retirement Income Review highlighted that Australia's pension system is unique compared to that of other countries[11]. Locally, our superannuation system is based on compulsory, privately managed funds with a large number of participants who are highly interconnected.

Sizeable

Superannuation funds are diverse, varying in size, complexity and target market. In addition, there is a high level of involvement of third parties who work on behalf of employers, members and funds.

Highly networked

Since the introduction of the superannuation guarantee in the early 1990s, the ecosystem continues to evolve in response to changes in its environment. In 2010, the Super System Review (Cooper Review) identified that the 'back office' of the superannuation industry was based on highly manual transactions and lacked industry data standards, inhibiting efficient processing of member accounts[12]. With the implementation of the SuperStream government package, the ecosystem now has a faster and digitised 'back office' environment compared to that in 2010. Examples of key SuperStream and associated reforms include the introduction of the Superannuation Data and Payment Standards in 2012 and the creation of the Superannuation Transaction Network in 2013 to transport contributions and rollovers between employers and superannuation funds. The STN currently processes approximately 165 million transactions per year[13].

$2.9 trillion in assets, one of the largest in the world. Of this total, 0.7 trillion are held by SMSFs[14]

165M
transactions per year processed by gateway providers[15]

24.4M
Member accounts[16]

+880K
Employers[17]

+593K
SMSFs[18]

1605
Small APRA funds[19]

Dynamic

Moreover, the superannuation ecosystem structure is in a constant state of flux. Regulatory focus on fund performance has driven various funds and trustees to merge or consolidate. The 1,511 superannuation organisations in 2004 had decreased to 207 in 2019[20].

Because of the economic impacts of the COVID-19 pandemic, in 2020 the Australian Government introduced changes that would allow eligible individuals to access their superannuation retirement savings earlier (as opposed to preservation age). From inception of this scheme on 20 April to 20 December, 3.4 million applications (one application could come from one of more members) were received and a total of $35.9 billion in payments were made – 44% of the applications were processed within 1–3 business days[21]. These figures show how quick the transactions were, with minimal time for detection and recovery of lost funds in the event of fraudulent activity.

Increased connectivity and engagement of superannuation organisations with third parties add entry points for threat actors and introduce additional complexity to securing the environment and building trust in the network. Other emerging conditions, such as the introduction of the New Payments Platform, Open Banking and the Consumer Data Right Rules, will continue to drive changes to how the ecosystem operates and the participants interact, and will potentially affect the ecosystem's overall cyber risk profile. With the expansion of digitisation, a data governance strategy and a secure framework for the use of open Application Programming Interfaces will be needed.

+300
Payroll providers[22]

101
Retail funds[23]

35
Industry funds[24]

25
Pooled superannuation trusts[25]

19
Public sector funds[26]

17
Corporate funds[27]

11
Custodians[28]

9
Gateway operators[29]

2
Major administrators

A fragmented yet evolving regulatory landscape

Is the current regulatory approach optimal?

The role of regulators is critical to building trust and cyber resilience. Is the current regulatory approach optimal for safeguarding the retirement savings of more than 24.4 million member accounts[30]?

Industry research suggests that 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[31].

Responsibility for governance of the Australian superannuation ecosystem is fragmented across multiple regulators. There are three main regulators: APRA, ASIC and the ATO. In addition, other entities, such as the Treasury, Australian Transaction Reports and Analysis Centre (AUSTRAC) and the GNGB regulate specific aspects of the ecosystem. The focus of the three main regulators (APRA, ASIC, ATO) is on particular outcomes across the financial system, not just superannuation. From a cybersecurity perspective, there is currently no single regulator responsible for governing cyber resilience across the superannuation ecosystem.

There are siloed and inconsistent cyber-regulatory expectations of entities across the superannuation ecosystem. APRA-regulated entities, such as funds, insurers and banks must comply with CPS 234. However, a large number of organisations and funds, such as SMSFs in the superannuation ecosystem, are not regulated by APRA nor are they required to have cybersecurity controls in place. SMSFs, for example, are not regulated by APRA and as of June 2019, collectively represent 26% of all super assets under management[32]. Between 2015 and 2020, the number of SMSF accounts has increased by 11.2 percent, and the number of APRA-regulated funds decreased by 28.5 percent[33]. The approach of focusing on bigger players and making individual organisations accountable for their own environments is no longer sufficient in a networked, co-dependent ecosystem.

In addition, even where standards exist for regulated entities, these are often principles based, leading to inconsistent interpretation and application across organisations.

Introduced requirements, such as APRA's CPS 234 Information Security Standard and the updated ATO DSP Operational Framework (for organisations who have digital interaction with the ATO), are meaningful strides towards closing the gap between superannuation regulation and digital reality. However, 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. Currently there are

What could be improved in existing regulatory frameworks and standards to enhance cyber resilience in the Superannuation industry?

92%
of respondents agreed that minimum common cybersecurity control baseline standards should be introduced industry-wide.

85%
of respondents agreed that existing frameworks and standards should be aligned and streamlined.

75%
of respondents agreed that frameworks and standards should be tailored to address industry specific development and threats.

> **"CPS 234 has been a benefit in focusing attention and budgets but compliance does not mean you are secure. To be secure, there are a core set of tasks, no matter how big you are."**
>
> Industry super fund representative

no specific requirements or clear guidance on areas such as managing cyber risk associated with third parties, cloud security, or cyber risk identification and quantification. Finally, 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.

The diagram on the right provides an indicative timeline of the key legislation, regulatory requirements and guidelines on cybersecurity applicable to the superannuation ecosystem. Note that the information in the timeline is not exhaustive.

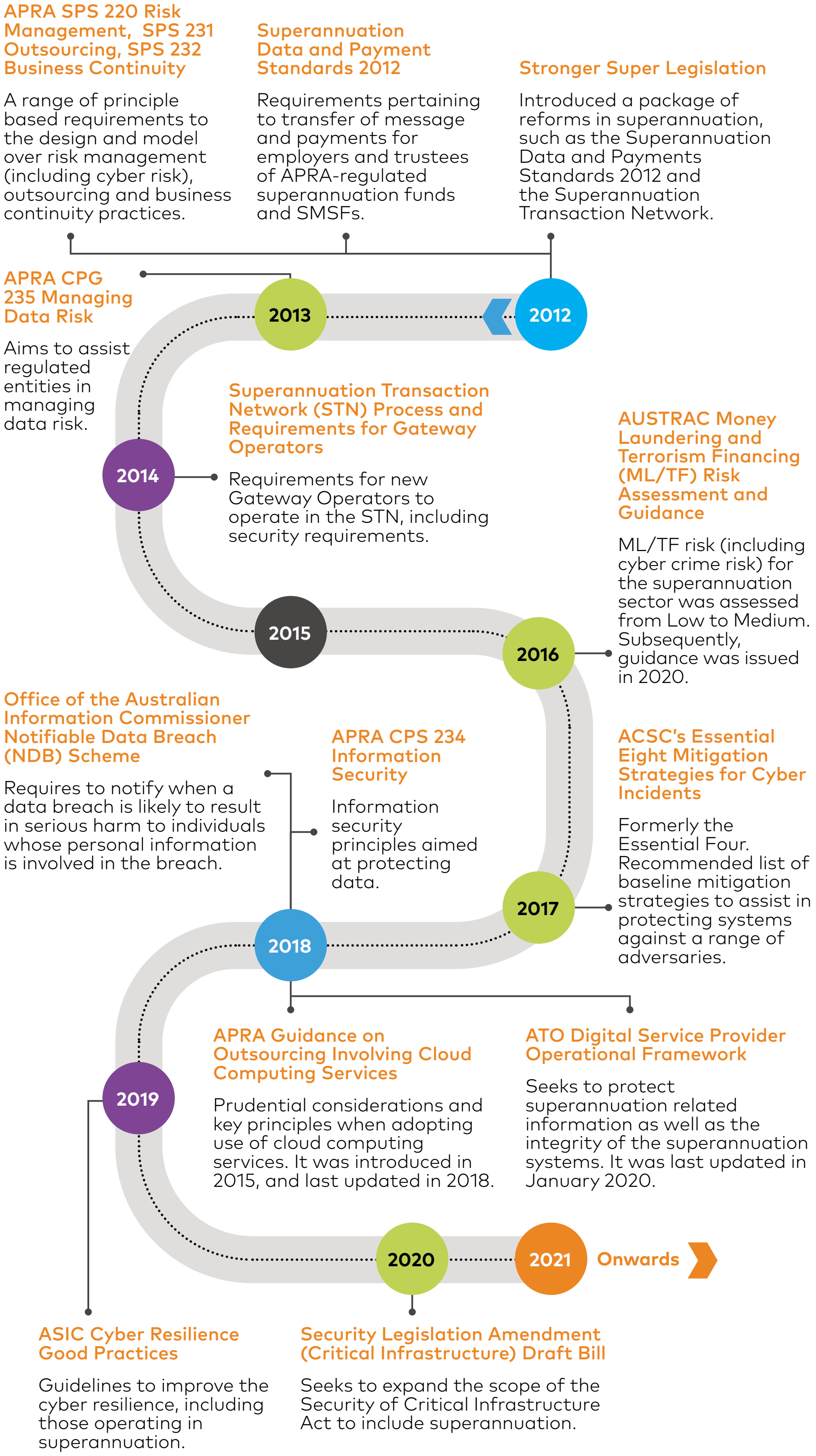
We understand that APRA is in the process of harmonising and consolidating some of its current prudential standards into cross industry standards which will be applicable to superannuation.

A strategy for cybersecurity in the Australian superannuation ecosystem

The unique characteristics of the Australian superannuation ecosystem distinguish it from other retirement systems overseas and from other industry sectors. In some countries, such as in Singapore, the national government manages the retirement savings of all workers through a single national fund. In contrast, the Australian superannuation ecosystem is sizeable, dynamic, highly networked and governed by multiple regulators.

However, although there is no other system that is directly

Regulatory timeline in the superannuation ecosystem



APRA SPS 220 Risk Management, SPS 231 Outsourcing, SPS 232 Business Continuity

A range of principle based requirements to the design and model over risk management (including cyber risk), outsourcing and business continuity practices.

Superannuation Data and Payment Standards 2012

Requirements pertaining to transfer of message and payments for employers and trustees of APRA-regulated superannuation funds and SMSFs.

Stronger Super Legislation

Introduced a package of reforms in superannuation, such as the Superannuation Data and Payments Standards 2012 and the Superannuation Transaction Network.

APRA CPG 235 Managing Data Risk

Aims to assist regulated entities in managing data risk.

Superannuation Transaction Network (STN) Process and Requirements for Gateway Operators

Requirements for new Gateway Operators to operate in the STN, including security requirements.

AUSTRAC Money Laundering and Terrorism Financing (ML/TF) Risk Assessment and Guidance

ML/TF risk (including cyber crime risk) for the superannuation sector was assessed from Low to Medium. Subsequently, guidance was issued in 2020.

ACSC's Essential Eight Mitigation Strategies for Cyber Incidents

Formerly the Essential Four. Recommended list of baseline mitigation strategies to assist in protecting systems against a range of adversaries.

Office of the Australian Information Commissioner Notifiable Data Breach (NDB) Scheme

Requires to notify when a data breach is likely to result in serious harm to individuals whose personal information is involved in the breach.

APRA CPS 234 Information Security

Information security principles aimed at protecting data.

APRA Guidance on Outsourcing Involving Cloud Computing Services

Prudential considerations and key principles when adopting use of cloud computing services. It was introduced in 2015, and last updated in 2018.

ATO Digital Service Provider Operational Framework

Seeks to protect superannuation related information as well as the integrity of the superannuation systems. It was last updated in January 2020.

ASIC Cyber Resilience Good Practices

Guidelines to improve the cyber resilience, including those operating in superannuation.

Security Legislation Amendment (Critical Infrastructure) Draft Bill

Seeks to expand the scope of the Security of Critical Infrastructure Act to include superannuation.

comparable, the learnings of other industries like the Australian energy sector may be applicable to the superannuation context.

Learning from the Australian energy sector

In 2018, industry and government stakeholders collaborated to develop a tailored cybersecurity framework for the Australian energy sector: the Australian Energy Sector Cyber Security Framework (AESCSF). The framework was a response to the recommendations from the 2017 Finkel Review Report (Independent Review into the Future Security of the National Electricity Market: Blueprint for the Future), which recommended the following to enhance cyber resilience in the energy sector:

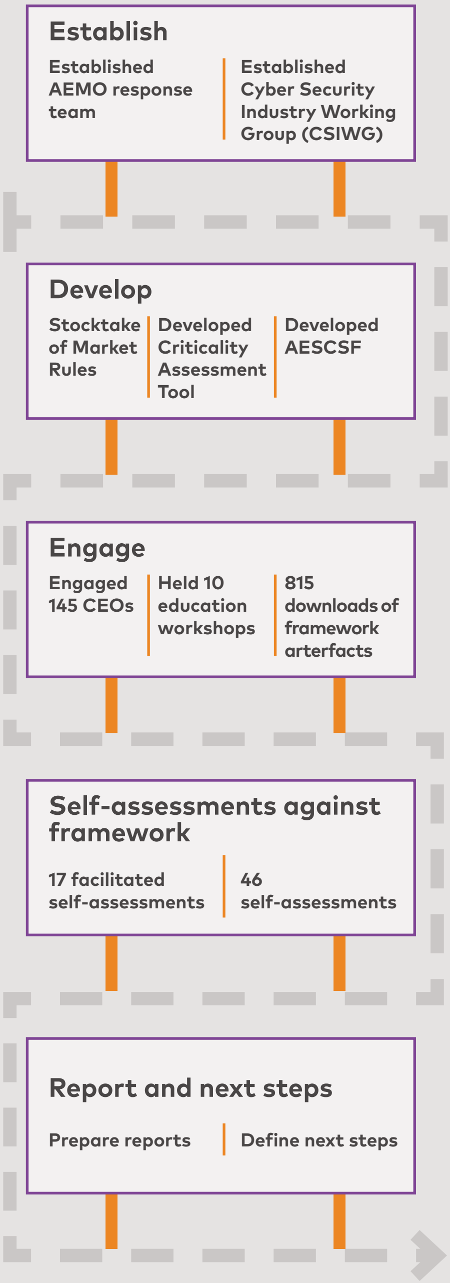
- An assessment of the cyber maturity of all energy market participants to identify and understand vulnerabilities;
- A stocktake of current regulatory procedures to ensure their sufficiency for potential cyber incidents in the National Electricity Market;
- An assessment of the Australian Energy Market Operator's (AEMO's) cybersecurity capabilities and third party testing; and
- An update from all energy market participants on how they undertake routine testing and assessment of cybersecurity awareness and detection, including requirements for employee training before accessing key systems.

The AESCSF provides a basis for energy sector participants to assess, in a standardised manner, their current state of cybersecurity capability and maturity. It also empowers participants to make informed decisions about what they need to do to become cyber resilient[34]. The framework is based on recognised industry standards, such as the National Institute of Standards and Technology's Cyber Security Framework (NIST CSF), ISO/IEC 27001 and Australian-specific control references, such as the ACSC's Essential Eight Strategies to Mitigate Cyber Security Incidents, the Australian Privacy Principles, and the NDB scheme.

The AESCSF has provided sector-wide visibility of the overall state of cybersecurity maturity across the energy sector, enabling the facilitation of coordinated efforts to better protect critical energy assets across Australia. In light of recently announced reforms to the Security of Critical Infrastructure Act, the AESCSF provides a leading example of a coordinated sector-wide effort, with collaboration across Government and Industry, to drive the cybersecurity agenda forward.

AESCSF Journey Overview

Summary of activities performed



Establish

Established AEMO response team

Established Cyber Security Industry Working Group (CSIWG)

Develop

Stocktake of Market Rules

Developed Criticality Assessment Tool

Developed AESCSF

Engage

Engaged 145 CEOs

Held 10 education workshops

815 downloads of framework arterfacts

Self-assessments against framework

17 facilitated self-assessments

46 self-assessments

Report and next steps

Prepare reports

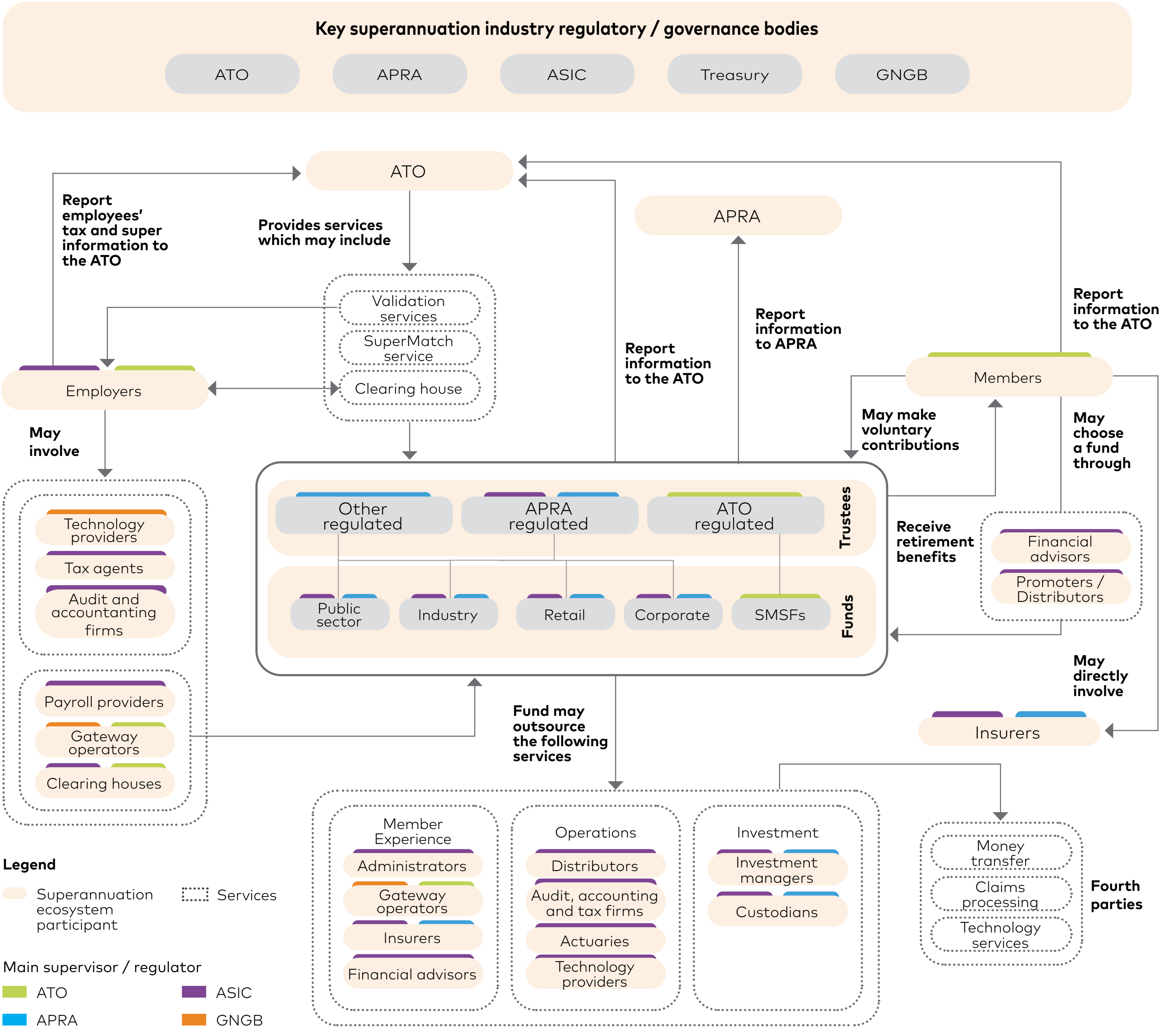
Define next steps

Key players in the superannuation ecosystem

The superannuation ecosystem consists of a large number of organisations, from some of the largest financial institutions in the country to over 880,000 employer organisations, some of whom are micro businesses in size. Accountants, bookkeepers, clearing houses, gateways, administrators and more make up the data supply chain. The image below provides an overview of the key players, including the main regulatory bodies, and illustrates the highly networked environment and the many possible integration points that comprise the ecosystem.

In such a complex and interconnected ecosystem, each organisation is a potential source of cyber vulnerabilities that can be introduced via a multitude of pathways. It is critical that all participants in this ecosystem play a part in collectively building cyber resilience across the ecosystem.

Superannuation ecosystem



Superannuation ecosystem - supporting notes

- Employers are required to pay the Superannuation Guarantee (SG) for eligible employees. To facilitate the payment of SG obligations to employee-nominated super funds, employers may engage third parties, such as payroll providers and clearing houses;
- Members receive their SG benefits from a superannuation fund, which may be selected by them or their employer. Members can make additional contributions to their superannuation fund either via their employers or directly into the fund. A superannuation member can generally access their fund once they reach retirement age. However, under certain circumstances some eligible members may withdraw some of their funds earlier (e.g. as a result of the Early Release Scheme implemented during the COVID-19 pandemic in 2020);
- If not selected by a member, a default 'MySuper' product and death and permanent disability insurance provider is selected via the employer;
- In Australia, superannuation funds operate under a trustee model in which the trustee has the ultimate responsibility for and the obligation to manage and protect their members' assets. There are three main types of funds that may be managed: Exempt Public Sector Superannuation Schemes (EPSSSs), APRA-regulated funds or SMSFs. APRA-regulated funds can be segmented in many ways but are generally classified into four types: public sector funds, industry funds, retail funds and corporate funds. Management of superannuation funds may involve third party services, such as administrators, distributors and investment managers; and
- The ATO plays a supervisory as well as operational role in the superannuation ecosystem. The ATO provides services, such as digital validation services. The ATO also offers a free clearing house service for small business employers.

A way forward: An industry, organisational and member approach to managing cyber risks

Cybersecurity is everyone's responsibility and, as such, everyone in the ecosystem has a role to play in addressing these challenges. In this section we describe the main challenges identified in our research and outline calls to system-wide action for consideration.

Challenge one: A lack of system accountability and cyber risk leadership

There is a lack of accountability for end-to-end cybersecurity resilience across the Australian superannuation system. Due to the ecosystems's complexity and highly networked environment, organisations, third parties and members do not always clearly understand their responsibilities.

Each organisation is ultimately accountable for their own environments and data (including the data managed by their service providers). Boards, in particular, are expected to demonstrate accountability for cybersecurity. There is an urgent need for cyber leadership with good understanding of cyber threats and of the importance of prioritising cybersecurity.

> **…Too many boards still lack visibility or understanding of the problems, while internal audit functions can lack the specialist skills to challenge boards and management to plug urgent gaps[35].”**
>
> Geoff Summerhayes, APRA Executive Board Member

Importantly, members don't often adopt behaviours to protect their money and data. Our research showed that individuals have an important role to play when it comes to cybersecurity. However, more education is needed to help them understand the ways in which cyber threats could compromise their personal information and retirement savings, and safeguard their future in the process (also refer to Challenge Three).

72%
of respondents indicated the ecosystem should work together to clarify accountabilities and responsibilities related to managing cyber risk.

62%
of survey respondents highlighted that limited understanding of cyber risk in senior management is a limitation for managing cyber risks. Leaders need to be able to drive a cyber risk–aware culture.

55%
of respondents agreed that there are unclear contractual requirements or expectations among related parties in relation to managing cyber risk.

Calls to action

Clarify roles and responsibilities to build cyber resilience

Industry leaders	Organisational leaders	Members / individuals
Government agencies, regulators and industry bodies that together govern the superannuation ecosystem.	Business leaders of organisations that participate in the superannuation ecosystem, including employers and organisations that provide services.	Superannuation members, employees and individuals who participate in the superannuation ecosystem.
Key considerations	**Key considerations**	**Key considerations**
• Define a framework that helps organisations in the system to clarify cybersecurity roles and responsibilities, which would inform a system-wide strategy for building resilience and a response to cybersecurity risks (e.g. define an ecosystem-wide responsibility assignment matrix or RACI); and • Define a consistent and practical approach to help those in the superannuation ecosystem to address third party security risks.	• Upskill on cybersecurity, drive a cyber risk–aware culture and commit resources to maintain a secure environment and protect their members; • Take responsibility for implementing and maintaining secure products and services, and protecting sensitive data (e.g. personal data of members/ employees); • Assess and manage cybersecurity risks when selecting service providers; and • Understand where critical information assets sit, their key threats and risks, including information assets and controls managed by third parties or related parties.	• Take accountability for their own data security and practice secure online behaviours, including (but not limited to): • Limiting the amount of personal information shared online or with unknown people and organisations; • Being suspicious of any requests for personal information or money transfers; and • Recognising and reporting cyber incidents.

Challenge two: Inconsistent cybersecurity capabilities

The superannuation ecosystem consists of a variety of organisations of different sizes and complexity. Organisations with weak cybersecurity capabilities are particularly vulnerable, ultimately posing a safety risk for the rest of the ecosystem.

Some participants in the ecosystem, such as smaller payroll providers, financial advisers and SMSFs have very basic capabilities, while others – like banks and global administrators – have specialised resources and more sophisticated processes and tools. In the 2020 ACSC Small Businesses Survey, almost half the Australian small and medium business respondents rated their cybersecurity understanding as 'average' or 'below average' and had poor cybersecurity practices[36].

In addition, competing business priorities in small- and medium-sized businesses represent a barrier to prioritising time and resources to the risk of cyber threats.

The lack of a requirement for a common minimum baseline of cyber controls also leads to inconsistent practices. While CPS 234 extends to the third and related parties of APRA-regulated entities, it does not extend to all organisations in the ecosystem and fourth parties. Non-APRA-regulated entities, such as tax agents and payroll providers, may engage with other third parties who are not required to comply with any specific cybersecurity requirements. In addition, various employer organisations, who send superannuation data and money into the ecosystem, are not subject to baseline security requirements.

> "
>
> **(The) number one (focus area) is to establish a baseline of cyber controls by reinforcing the embedding of non-negotiable cyber practices, facilitating better sharing of cyber information and enabling more effective incident response processes. It's close to 18 months since CPS 234 came into effect, and we are still seeing too many basic cyber hygiene issues across the industry[37]."**
>
> Geoff Summerhayes, APRA Executive Board Member

Business leaders need to place cybersecurity at the forefront of their business strategy. Our research shows allocation of resources to mitigate cyber risks has started to increase – this focus needs to continue at pace.

Cybersecurity is not normally a key consideration for members, as they often select funds based on performance and/or fees. Therefore, funds do not often see cybersecurity as a competitive differentiator.

Calls to action

The ecosystem needs to get the basics right

Industry leaders

Government agencies, regulators and industry bodies that together govern the superannuation ecosystem.

Key considerations

- Define a minimum and common baseline of cybersecurity controls ecosystem-wide in consultation with all stakeholders, that are:
  - Clear and specific; and
  - Practical for organisations of different size and complexity to implement.

  Examples can be obtained from frameworks used in other industries, such as the AESCSF or the Australian Government's Strategies to Mitigate Cyber Security Incidents (including the Essential Eight mitigation strategies)[38].
- Enforce and monitor industry adherence through a defined mechanism (e.g. attestation or certification process).

Note:
The 2020 Australia's Cyber Security Strategy will prioritise support for small- to medium-sized enterprises through a number of initiatives, including the ACSC Small Business Cyber Security Guide, ACSC-produced Step-by-Step Guides and Quick Wins for Small Business[39].

Organisational leaders

Business leaders of organisations that participate in the superannuation ecosystem, including employers and organisations that provide services.

Key considerations

- Place cybersecurity at the forefront of business strategy;
- Plan for skilled resources, processes and tools to meet requirements for baseline controls;
- Monitor the operating effectiveness of baseline controls across the business network; and
- Assess your third parties' adherence to baseline controls.

Members / individuals

Superannuation members, employees and individuals who participate in the superannuation ecosystem.

Key considerations

- Ask service providers how they are protecting your data and consider cybersecurity risks when selecting your service provider (e.g. privacy protection and security features, such as Multi-Factor Authentication (MFA) and transaction notifications);
- Protect your electronic devices and information by following the latest advice from relevant trusted sources, such as the ACSC and Scamwatch. At a minimum:
  - Use strong unique passwords online and enable MFA;
  - Keep software up to date by installing the latest patches (e.g. operating systems, web browsers and plugins like Java); and
  - Don't access/provide sensitive information (e.g. access online banking, superannuation account or make credit card payments) when using public computers or accessing public wi-fi.

Challenge three: Low levels of cyber awareness

Research shows individuals are often considered the weakest link in managing cyber risk. If cyber resilience across the ecosystem is to be strengthened, all individuals, especially members, need to be educated about cyber risks and potential impacts on their retirement savings.

More than half of our survey respondents (54%) indicated that members infrequently checking their accounts is a main factor that drives cyber risk. By design, superannuation members engage with their superannuation accounts less frequently than they do with their bank accounts; that is, mostly until they near retirement age. In addition, some features, such as MySuper and insurance protection, are selected by default so there is little incentive for members to make considered choices and understand their implications. The lack of understanding about super and the lack of interaction with superannuation accounts affects the timely identification of illicit or erroneous activity.

Accountability for the compensation of financial loss from unauthorised access to a member's retirement savings is currently unclear and determined on a case-by-case basis. Clarity is needed on who is responsible when compromised credentials are used to access a member's account without authorisation. Members need to be made aware that they are responsible for keeping their information and credentials confidential. They should also be made aware that when their retirement savings are stolen, they may not be reimbursed in all circumstances.

Moreover, some members are unaware of cyber risks and basic cyber hygiene practices, such as the enablement of multi-factor authentication and the use of strong and unique passwords.

Calls to action

Influence members' cyber awareness, education and practices

Industry leaders	**Organisational leaders**	**Members / individuals**
Government agencies, regulators and industry bodies that together govern the superannuation ecosystem.	Business leaders of organisations that participate in the superannuation ecosystem, including employers and organisations that provide services.	Superannuation members, employees and individuals who participate in the superannuation ecosystem.
Key considerations	**Key considerations**	**Key considerations**
Collaborate to design and deliver cyber awareness and education campaigns targeted at members.	• Collaborate on cyber awareness campaigns and cyber education plans for all individuals in the ecosystem including members; • Implement strong authentication techniques, such as multi-factor authentication; • Prompt members to enable strong security settings through their online portal or application features; and • Communicate to members of the potential cyber risks and threats through different distribution channels, such as email communications, application notifications and call centre interactions.	Know where to go for information about cyber threats: refer to available online resources, such as the ACSC website to learn about: • Cyber threats and risks; • How to better protect your personal and financial information online; and • How to report a suspicious event (e.g. scam, phishing, identity theft).

Challenge four: Barriers to sharing threat intelligence

As the scale and sophistication of cyber threats continue to escalate, threat intelligence is key to understanding and mitigating cyber risks.

Our research shows that information about threats are shared between different pockets of the ecosystem, such as the Joint Cyber Security Centres (JCSC), Australian Financial Crimes Exchange (AFCX), Financial Services Information Sharing and Analysis Center (FS-ISAC), as well as other informal groups in specific sectors. However, most organisations in the superannuation ecosystem do not have a formal platform or forum for sharing threat information in a confidential and secure manner. Our respondents indicated that while there have been previous attempts to set up threat-sharing platforms, these have been unsuccessful.

In our survey, more than half of the survey respondents (58%) indicated that barriers to sharing threat information is a main challenge in managing cyber risks in the superannuation ecosystem. Business leaders, ecosystem regulators and industry bodies need to work together to understand and address these barriers.

Barriers to sharing cyber threats, uncovered through our research, include the following:

- The lack of an accountable entity in the ecosystem who coordinates threat sharing;
- Organisations that are reluctant or unwilling to share threat information because they do not believe the environment is sufficiently safe for sharing; and
- Small- to medium-sized organisations don't tend to have dedicated and/or skilled resources to identify and act upon threat information.

Lessons from other cyber threat-sharing forums, such as the United Kingdom's (UK's) Cyber Security Information Sharing Partnership (CiSP), may be leveraged to establish an approach that is optimal and tailored for Australian superannuation. CiSP is a joint industry and government initiative run by the UK National Cyber Security Centre to allow UK organisations to share cyber threat information in a secure and confidential environment. Registration to the initiative is free and membership includes the following benefits:

- Ability to engage with industry and government counterparts in a secure environment;
- Early warning of cyber threats;
- Ability to learn from experiences, mistakes, successes of other users and to seek advice;
- An improved ability to protect the company's network; and
- Access to free network monitoring reports tailored to an organisation's requirements[40].

Calls to action

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

Industry leaders	Organisational leaders	Members / individuals
Government agencies, regulators and industry bodies that together govern the superannuation ecosystem.	Business leaders of organisations that participate in the superannuation ecosystem, including employers and organisations that provide services.	Superannuation members, employees and individuals who participate in the superannuation ecosystem.
Key considerations	**Key considerations**	**Key considerations**
• 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; • Provide a secure platform in which to share information; and • Co-develop cyber-detection strategies that ecosystem participants can use (e.g. red teams, attack simulations).	• Join partnerships to share threat information in a secure and confidential manner. Understand and know how to act on that information; • Leverage or expand on existing resources to analyse and monitor threat information; and • Develop threat models for defence and recovery strategies.	• Monitor accounts more frequently and report suspicious events or potential threats (e.g. phone/sms scams, phishing emails); • Activate notification settings to receive alerts of financial (e.g. fund transfer) and non-financial (e.g. change of personal details) transactions on your account; and • Sign up for regular threat alerts (e.g. ACSC's Alert Service, Scamwatch alert emails).

Challenge five: The lack of a holistic cybersecurity resilience strategy

There is no body that is clearly accountable for the coordination of cybersecurity response and recovery strategies across the superannuation ecosystem. There are some groups in the ecosystem that perform coordinated response testing, such as gateway operators. But an overarching incident response plan is missing and to date, an ecosystem-wide incident response testing covering multiple entities has yet to be performed.

Yet, the majority of our survey respondents indicated that the ecosystem should work together to co-develop detection (75%) and response (87%) strategies for incidents that directly affect multiple organisations. Examples from other industries may be leveraged for this purpose, such as the North American Electric Reliability Corporation's (NERC) grid security exercise (GridEx) and incident response testing.

Led by the NERC Electricity Information Sharing and Analysis Center (E-ISAC), GridEx provides a forum to demonstrate how participants would respond to and recover from coordinated cyber threats and incidents. It also offers opportunities for organisations to strengthen crisis communications and relationships and provide feedback for lessons learned during the exercise. In 2019, GridEx V included more than 500 organisations, comprising utilities, government and law enforcement agencies and other organisations. In addition, more than 100 executives and staff members from the electricity industry, its cross-sectoral partners and government attended the Executive Tabletop to share additional perspectives on critical security policy issues. Participation has broadened among interdependent industries and governmental organisations from the United States, Canada, Mexico, New Zealand, Australia, and the United Kingdom[41].

Calls to action

Co-develop cyber response and recovery strategies

Industry leaders	Organisational leaders	Members / individuals
Government agencies, regulators and industry bodies that together govern the superannuation ecosystem.	Business leaders of organisations that participate in the superannuation ecosystem, including employers and organisations that provide services.	Superannuation members, employees and individuals who participate in the superannuation ecosystem.
Key considerations	**Key considerations**	**Key considerations**
Define a dedicated superannuation cyber-governance body to help coordinate response and recovery testing from incidents affecting multiple organisations across the value chain.	• Participate and co-develop cyber response and recovery strategies; • Participate in incident response planning and testing exercises; and • Continuously improve cybersecurity capabilities in response to lessons learned and changes in the threat environment.	• Know where to go to remain up to date with the most common online security risks and with practical advice on how to protect yourself (e.g. visit the ACSC website for individuals and families); and • Report suspicious events to your financial institution and applicable authorities (e.g. ReportCyber, Scamwatch, IDCare, local police). If you think your credentials have been stolen, act quickly. Notify the suspicious event to the relevant institution and parties and change your passwords.

Conclusion

Superannuation plays a crucial part in securing the future of working and retired people in Australia.

As we have seen, the complexity of the superannuation system in Australia, coupled with the rate at which the cyber threat landscape is evolving, introduces serious cyber risks – and leaves members, organisations, business partners, and the ecosystem itself vulnerable. Our research indicated not all organisations within the ecosystem have implemented essential cyber defences, aren't as educated about cyber risk as they should be and that many members don't act proactively enough to protect their retirement.

But we can counter this systemic risk. Small measures such as minimum and standardised cybersecurity controls, a clear and transparent system for sharing cyber intelligence, and a well-rehearsed approach to responding to incidents can make a big impact on safeguarding members' superannuation savings and protecting our superannuation system.

Securing the future of the Australian superannuation ecosystem against cybersecurity threats is a critical responsibility, one we can address together. When it comes to taking meaningful action, there has never been a better time.

Participants

The insights from this report were obtained from interviews with key representatives across the superannuation ecosystem, supported by a survey completed by a broad range of stakeholders in the ecosystem, consultation with superannuation subject matter experts (SMEs), and broader industry research.

Interviewed ecosystem stakeholders

Interviewees included senior business and cybersecurity executives from the following participant organisations in the superannuation ecosystem:

- Administrator
- Custodian
- Clearing house
- Employer
- Gateway operator
- Industry body / association
- Industry superannuation fund
- Public sector superannuation fund
- Retail superannuation fund
- Payroll provider
- Regulatory bodies
- Technology vendor

Surveys

Breakdown of respondents by entity type roles

- Administrator (35%)
- Actuary (4%)
- Clearing house (24%)
- Custodian (6%)
- Employer (24%)
- Financial adviser (18%)
- Gateway operator (30%)
- Insurer (10%)
- Investment manager (17%)
- Payroll service provider (8%)
- Corporate superannuation fund (13%)
- Industry superannuation fund (34%)
- Public sector superannuation fund (11%)
- Retail superannuation fund (7%)
- Technology vendor (18%)
- Trustee (21%)
- Other (14%)

As one organisation may have one or more roles in the ecosystem, survey respondents represent one or more organisation types.

Size of respondent's organisation

- 1–10 employees (7%)
- 11–50 (11%)
- 51–200 (30%)
- 201–500 (17%)
- 500–1500 (17%)
- 1500+ (18%)

Respondent's role

- Board member (4%)
- C-level (Executive management) (23%)
- Mid/Senior management (48%)
- Staff/Specialist (23%)
- Other (3%)

Respondent's work domain

- Business operations (11%)
- Finance (4%)
- Risk management (20%)
- Information technology (37%)
- Cybersecurity (17%)
- Other (11%)

References

1 Prime Minister of Australia (2020), Statement of Malicious Cyber Activity Against Australian Networks 19 June 2020, at https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks

2 ACSC (2020), ACSC Small Business Survey Report: How Australian Small Businesses Understand Cyber Security, at https://www.cyber.gov.au/acsc/view-all-content/news/announcing-acsc-small-business-survey-report

3 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

4 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

5 APRA (2020), The superannuation Early Release Scheme: Insights from APRA's pandemic data collection, APRA Insight – Issue Four 2020, at https://www.apra.gov.au/superannuation-early-release-scheme-insights-from-apra%E2%80%99s-pandemic-data-collection.

6 New Zealand's Exchange (2020), Connectivity Issue Memorandum, 26 August 2020, at https://www.nzx.com/announcements/358636.

7 ACSC (2020), ACSC Annual cyber threat report: July 2019 to June 2020, at https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf.

8 ACSC (2020), ACSC Annual cyber threat report: July 2019 to June 2020, at https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf.

9 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

10 ACSC (2020), ACSC Annual cyber threat report: July 2019 to June 2020, at https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf.

11 Commonwealth of Australia (2020), Retirement income review: Final report, at https://treasury.gov.au/sites/default/files/2020-11/p2020-100554-complete-report.pdf.

12 Commonwealth of Australia (2010), Super system review: Final report, at https:/ /treasury.gov.au/publication/super-system-review-final-report.

13 GNGB (2021), Transaction data, as of 31 October 2020.

14 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

15 GNGB (2021), Transaction data, as of 31 October 2020.

16 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

17 Australian Bureau of Statistics (2019), Counts of Australian Businesses, including Entries and Exits, at https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/june-2015-june-2019.

18 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

19 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

20 APRA (2021), Superannuation in Australia: A timeline, at https://www.apra.gov.au/superannuation-australia-a-timeline.

21 APRA (2021), COVID-19 Early Release Scheme – Issue 35 accessible version, at https://www.apra.gov.au/covid-19-early-release-scheme-issue-35-accessible-version.

22 ATO (2021), Products register, at https://softwaredevelopers.ato.gov.au/product-register#Functionality=*Payroll%20(STP).

References

23 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

24 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

25 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

26 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

27 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

28 Australian Custodial Services Association (2020), Assets under administration for periods ending 31 Dec 2019 and 30 June 2020, at https://acsa.com.au/page/AssetsUnderAdmin

29 GNGB (2021), List of gateway operators, at https://www.gngb.com.au/gateway-operators-listing/.

30 APRA (2021), Annual superannuation bulletin: June 2015 to June 2020 - superannuation entities, Issued 29 January 2021, at https://www.apra.gov.au/annual-superannuation-bulletin.

31 Productivity Commission (2018), Superannuation: Assessing efficiency and competitiveness, Productivity Commission Inquiry Report No. 91, at https://www.pc.gov.au/inquiries/completed/superannuation/assessment/report/superannuation-assessment.pdf.

32 ATO (2020), SMSF profile, at https://www.ato.gov.au/about-ato/research-and-statistics/in-detail/super-statistics/smsf/self-managed-super-funds--a-statistical-overview-2017-18/?page=2#fn1.

33 APRA (2021), Annual superannuation bulletin - highlights June 2020, released 29 January 2021, at https://www.apra.gov.au/sites/default/files/2021-01/Annual%20superannuation%20bulletin%20highlights%20-%20June%202020_0.pdf.

34 Australian Energy Market Operator Limited (2019), Australian Energy Sector Cyber Security Framework (AESCSF), at https://aemo.com.au/-/media/files/cyber-security/2019/aescsf-framework-overview.pdf?la=en.

35 Summerhayes, G. (2020), Executive Board Member Geoff Summerhayes – speech to Financial Services Assurance Forum, 26 November, at https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services

36 ACSC (2020), Cyber security and Australian small businesses: Results from the Australian Cyber Security Centre Small Businesses Survey, at https://www.cyber.gov.au/sites/default/files/2020-07/ACSC%20Small%20Business%20Survey%20Report.pdf.

37 Summerhayes, G. (2020), Executive Board Member Geoff Summerhayes – speech to Financial Services Assurance Forum, 26 November, at https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services

38 ACSC (2020), Essential Eight Explained, at https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Essential%20Eight%20Explained%20%28June%202020%29.pdf.

39 Department of Home Affairs (2020), Australia's Cyber Security Strategy 2020, at https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

40 UK National Cyber Security Centre n.d., Keep up to date: CiSP, website, at https://www.ncsc.gov.uk/section/keep-up-to-date/cisp#section_3.

41 North American Electric Reliability Corporation (NERC) n.d., GridEx, at https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx.

Contact us to find out more

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

Michelle Bower
Executive Officer
GNGB
michelle.bower@gngb.com.au

Peter Malan
Partner
Cybersecurity & Digital Trust
PwC Australia
peter.malan@pwc.com

About GNGB

The Gateway Network Governance Body Ltd (GNGB) is a body that governs the Superannuation Transaction Network (STN) and supports the superannuation ecosystem. The GNGB is a not-for-profit organisation whose main purpose is to manage the integrity of the STN by undertaking initiatives to promote the efficiency and effectiveness of the STN, monitoring compliance with the Standards, managing new entrants to the network, and engaging with key stakeholders in government and the ecosystem.

For more information, visit www.gngb.com.au

About PwC Australia

In an increasingly complex world, PwC works with businesses, government and the community to help Australia continue to thrive and grow. Our purpose is to build trust in society and solve important problems, and we believe the most important problems are better solved together.

PwC is an active participant in the superannuation industry. We advise clients on every aspect of the superannuation industry from emerging risks and opportunities, regulatory compliance to mergers and acquisitions, with specialists in assurance, actuarial, tax, risk management and compliance, services for private clients, strategic advice, investments, technology and forensics.

PwC is at the forefront of thought leadership and lobbying on issues that affect the superannuation industry.

Gateway
Network
Governance
Body