Deloitte.

Superannuation Sector

How the Super sector can protect its members' whilst navigating cyber challenges

2023 Edition

Introduction

The cyber security threat landscape is becoming more sophisticated with the attack surface expanding. While the evolution of technology has created significant space for innovation and efficiency in the workplace, this innovation has also unlocked huge opportunity for cyber attackers, including those less skilled, to leverage advanced techniques and tools to compromise systems and cause devastating impacts to business operations and reputations. This heightened cyber risk is especially pertinent to the Super sector, who are caretakers for vast amounts of personal data and as an industry hold more than $3.3 trillion in member assets[1].

In addition to the change in and exacerbation of cyber threat, the super sector is also trying to juggle complex and evolving technology, business and regulatory environment, which includes a high level of market consolidation activity.

One of the most significant regulatory changes for superannuation trustees has been the introduction of the Australian Prudential Regulation Authority (APRA), Prudential Standard CPS 230 – Operational Risk Management. CPS 230 expects superannuation trustees to meet enhanced requirements with respect to the management of operational risk, business continuity, and service providers. Together with CPS 234, the related Prudential Standard on Information Security, it forms APRA's proposed new operational resilience framework for the financial services institutions it regulates.

To meet these revised operational resilience requirements and the broader threat challenges, it is imperative that superannuation trustees review their cyber security frameworks as they relate to internal operations and third- and fourth-party services providers. Frameworks need to ensure the robust and sustainable management of cyber risks, not only as they relate to the superannuation organisation but also as they relate to the strategic outcomes for superannuation members.

Without an earnest shift in focus to what is important – having cybersecurity capabilities that align with their business' risk appetites and fulfil their regulatory obligations – superannuation trustees face the very real risk of financial and reputational shortfall.

In this paper we will examine some of these key changes and security challenges the super sector is facing. Taking lessons learnt from recent incidents, we propose steps for how organisations can better protect themselves and the financial interests of their members.

[1] https://www.apra.gov.au/news-and-publications/apra-releases-superannuation-statistics-for-september-2022

What Has Changed In Recent Years:
Digital Transformation

In recent years, almost every industry has undergone major digital transformation. This has been the result of two things: rapid technological advancements – which have created a need to keep up – and an increased opportunity to integrate digital capabilities for business competitiveness. For the Super sector, both of these drivers have been guiding a transformation to adopting cloud technologies.

A cloud migration involves a company moving, in part or in full, its digital assets, services, databases, IT resources or applications into a cloud service provider's infrastructure. To date, many in the industry have adopted hybrid models where their infrastructure is split between on-premises and the private or public cloud. Cloud migrations can offer many benefits, from cost-reduction to scalability, availability, and security; but as with any transformational technology, it also brings new potential risks.

As nearly half of all data breaches in 2022 happened in the cloud, it is not necessarily as secure as it might seem, the average cost of a breach for organisations with a private or public cloud presence was millions of US dollars.

Decisions to migrate assets and capabilities to the cloud are thus important and organisations need to take steps to ensure that information and system security is being managed appropriately, even where responsibility for them is shared with cloud service providers.

What Has Changed In Recent Years:
Changing Business Environment

The Super industry is simultaneously seeing a shift in its technology and business operating model, and an increased reliance on service providers, which in turn has meant increased supply chain complexity, especially as more cloud and SaaS services are onboarded as critical assets. These factors are changing the business environment in which Superannuation organisations operate, and how theirs and their customers' data must be protected.

This uplift in use of service providers, though undoubtedly having brought value as fund members have more access to efficient services, has increased the requirements and expectations for trustees to manage third party relationships, particularly in terms of cybersecurity. The important data that trustees hold for their members is more challenging to protect, exposing them more to cyber risk. The burgeoning of cyber capability of cyber threat actors, coupled with the recent condemnation of companies deemed to have failed in protecting their customers' information details, mean that ensuring appropriate information security is more essential than ever before.

What Has Changed In Recent Years:
Changing Business Environment

The supply chain is already a common attack vector targeted by cyber criminals. By outsourcing more, a trustee's attack surface is widened, increasing the potential for cyber criminals to gain access to and exploit a company's resources. This attack vector can be seen in the Australian financial industry in recent cases whereby an attacker used a third party vendor to access login credentials, causing system compromise. By extending the ways in which a company can be breached, cyber security becomes more complex, leading to more incidents within the industry.

Whilst relinquishing outsourced services may not be the answer, superannuation funds should take steps to assess and ensure the suppliers they utilise have sufficient information security controls in place. Further, identity management should be leveraged to ensure both role-based and privileged access are appropriately managed to protect organisations against privilege escalation attacks through third-party systems. Alternatively, taking services fully in-house allows a fund to take full control of their members' journeys. This would be a significant strategic undertaking for superannuation trustees, with an estimated $250 million[2] annual cost for technology, with planning and consideration needing to be made for the protection of member data and privacy. There are pros and cons to both instances, but in either case, it is imperative that Super funds understand the business environment in which they function, the way that their organisation is operating, and how best their members' data should be managed and protected.

[2] https://www.smh.com.au/business/banking-and-finance/why-top-super-funds-are-taking-admin-in-house-20201030-p56a6v.html

What Has Changed In Recent Years:
Information Security Regulation

APRA's Prudential Security Standard (CPS234) has enhanced the regulatory obligations that the Super industry is subject to, mandating trustees to implement requirements to improve their security postures. Trustees must fully understand these requirements to both ensure compliance against their obligations, but also to support and improve their information security postures. CPS234 aims to holistically uplift an organisation's cybersecurity with a focus on the governance and risk management of information security. Despite its ambitious reach, the regulation does not have specific steps to achieve compliance, making it often ambiguous to understand and therefore difficult to effectively achieve.

Broadly speaking, CPS234's requirements include:

01

Framework
Maintain a comprehensive information security policy framework.

02

Roles and Responsibilities
Clearly define information security roles and responsibilities for the Board, senior management, governing bodies and individuals. It is stated that the board of an APRA-regulated entity is ultimately responsible for ensuring information security.

03

Controls Implementation
Robust information security controls must be in place and consider vulnerabilities, threats and asset criticality.

04

Third Party Compliance
Ensure third parties have similar information security policies and practices in order to protect the sensitive information and assets of the trustee.

05

Systematic Assurance
Continually test systems to ensure information security capabilities evolve with the changing threat landscape.

06

Information Asset Classification
Classify information assets according to their criticality and sensitivity. This includes those managed by third parties.

07

Security Incident Response
Incident response mechanisms must be in place to detect and respond to information security incidents in a timely manner. In addition, information security response plans must be annually reviewed to ensure they remain effective.

08

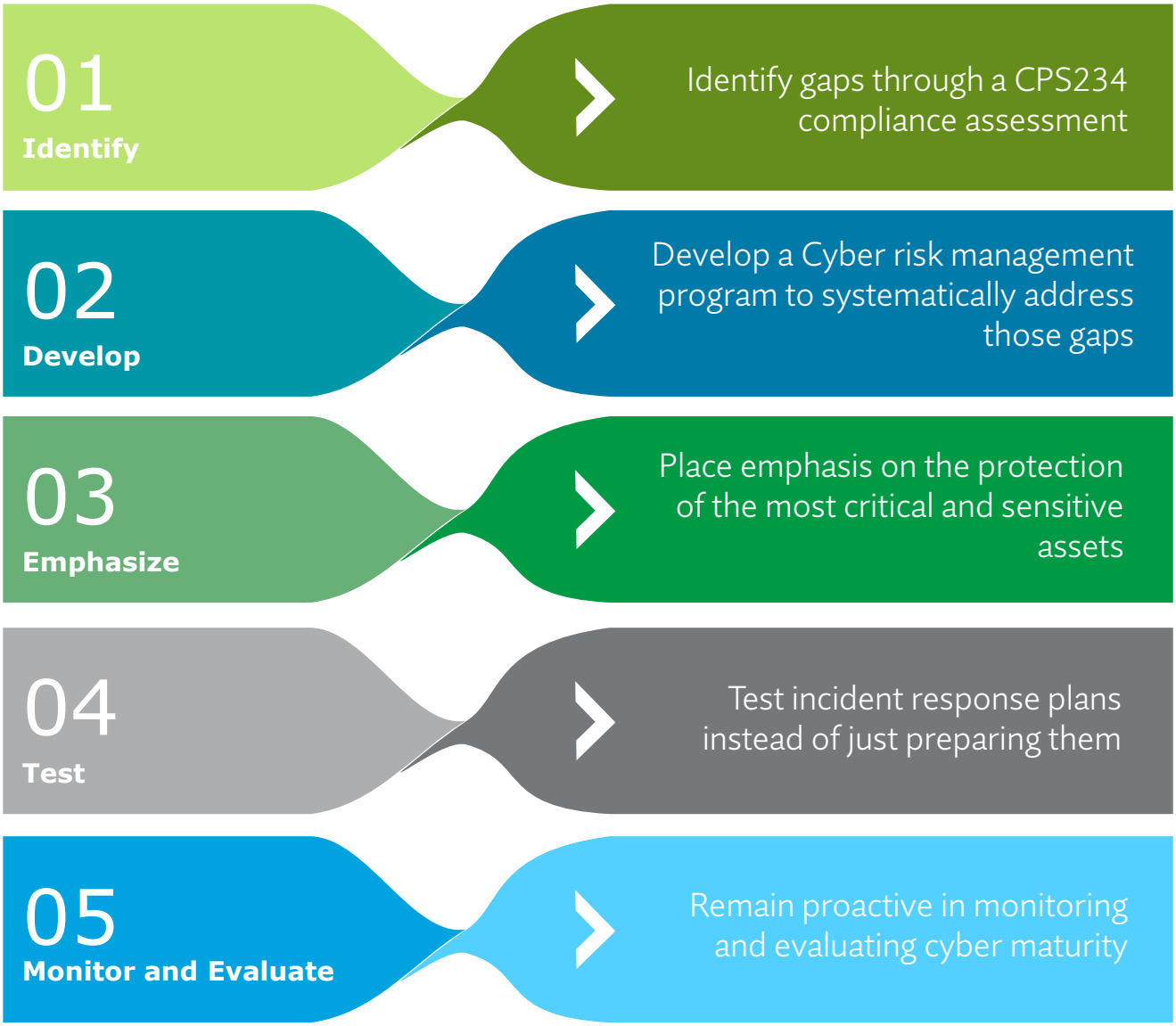
Internal Audit
A review of the design and operating effectiveness must be conducted, including those of third parties.

09

APRA Notification
It requires a timely response (within 72 hours) to APRA in the event of a data breach or security incident.

Adhering to CPS234

To ensure effective compliance with CPS234, there are a few steps that organisations can take:



APRA are also mandating all regulated entities to undertake an independent external assurance review of their compliance with CPS234 ("tripartite reviews"). Effectively preparing for these through readiness and Internal Audit reviews is essential and entities should ensure that they have effective plans in place to address known gaps to compliance.

The Evolving Cyber Landscape:
Complex Changes in Cyber Threats and Risk in Parallel

Last but certainly not least, the complexity and sophistication of cyber threat actors and threats are rapidly increasing, with a corresponding exacerbation of the impact of these threats and attacks. From the ACSC's 2021-22 Annual Cyber Threat Report, the following threats can be assessed as the most relevant to the Super sector, due to the volume of attacks, as well as the detrimental impacts that would result from such an incident:

Cyber-enabled Fraud
Cyber enabled fraud made up for 26.9% of the 76 000 reported cases. Notable incidents of cyber fraud being committed in superannuation include the SMSF Rollover schemes and the 2020 Covid-19 Early Release scheme which saw superannuation members lose more than $2 million and $120 000 respectively. Financial crimes are not a surprise with the large monetary incentives and access to digital means of exploitation.

Business Email Compromise (BEC)
Business email compromise made up a total of 6.12% of the reported cases. Business email compromise was not only limited to malicious actors compromising employee emails to extract funds, but confidential information was also targeted. The average loss per BEC was $64 000 and the compromise of a single email can also be the prelude to a ransomware attack.

Ransomware
Ransomware made up 0.59% of the reported cases. Despite the relatively smaller number of reported incidents, the ACSC assesses that ransomware remains the most destructive cybercrime threat. Ransomware is expensive to resolve from all angles, with the average cost of one being USD $4.54 million in 2022[3] which doesn't include the ransom. In consideration of the cost of the ransom, the costs from lost productivity due to system.

Despite not being unique to superannuation, these threats present major challenges to superannuation funds trying to protect their members' financial and data assets.

Importantly, while cybercrime capabilities have become more sophisticated, they have also become more accessible. The proliferation of cybercrime-as-a-service means that organisations should stay vigilant in their cybersecurity programs regardless of their threat profile.

The complexity of the types and breadth of threats that trustees are exposed to, especially in conjunction with the rapidly changing environmental factors, creates significant opportunity for cyber attackers and a significantly increased cyber risk for the industry with potentially catastrophic consequences, if not managed effectively.

[3] https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf

Lessons Learnt from Prior Incidents:
How Can the Industry Protect Itself?

With the combined changes in both the business and cyber landscapes, it is important to assess previous incidents to shape the industry's strategy for ensuring that sufficient controls are in place for the future. There are numerous past incidents that can be analysed to understand the factors that made the incident possible, to learn what additional controls that an organisation could implement to minimise the possibility and impact of a similar incident happening to them.

Taking cyber fraud as an example, it has become an increasingly serious issue in superannuation, with many cases having seen Australian Federal Police involvement. In a 2019 case, a 21-year-old Melbourne woman was arrested as being part of a large-scale online syndicate that stole millions of dollars from their victims' superannuation and trading accounts[4]. They used stolen information purchased from the dark web to commit fraud and identity theft, opening fake bank accounts that can access the legitimate ones of their victims. Cases like these show the far-reaching consequences of data breaches on financial systems.

Another incident type is Phishing, which remains the biggest threat for superannuation to date. The industry has seen many cases of compromised member credentials through phishing attacks that have lead to fraud. Successful phishing attacks often result in cyber criminals obtaining a user's log in details and leveraging this to break into the organisations systems. It has been proven that phishing is a prevalent threat in the Australian Super sector. A recent attack saw thousands of member records compromised, and personal information such as names, addresses, age, super account numbers, and balances stolen, as a result of an employee clicking a malicious link contained in a phishing email. In evaluating cases such as this one, trustees can assess their own policies and processes to implement further steps to help ensure security for their own members.

[4] https://www.afp.gov.au/news-media/media-releases/online-fraud-syndicate-dismantled-after-allegedly-siphoning-millions

Lessons Learnt from Prior Incidents:
How Can the Industry Protect Itself?

Some critical steps in addressing the risk of phishing include:

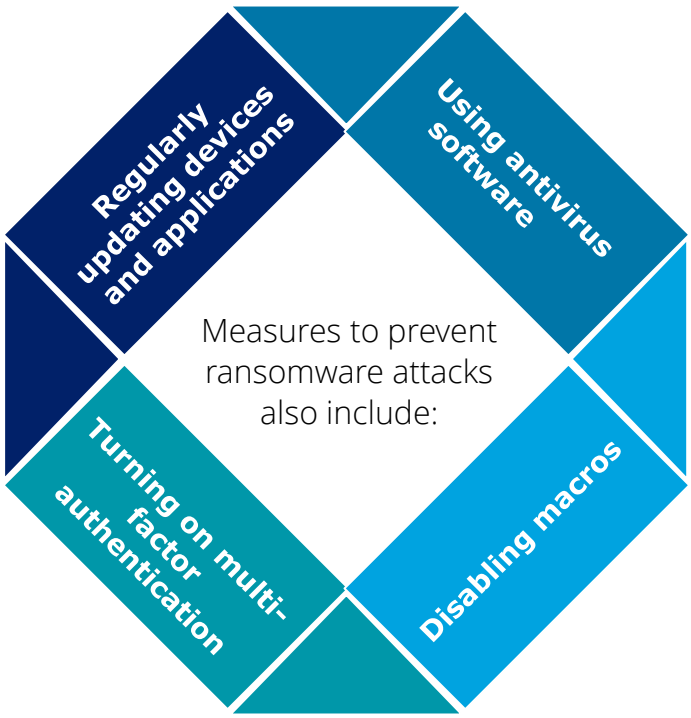
- Increasing security awareness among employees and members and,
- Enabling multi-factor authentication, can help reduce the number of successful phishing attempts. Doing so will in turn protect members' financial interests.

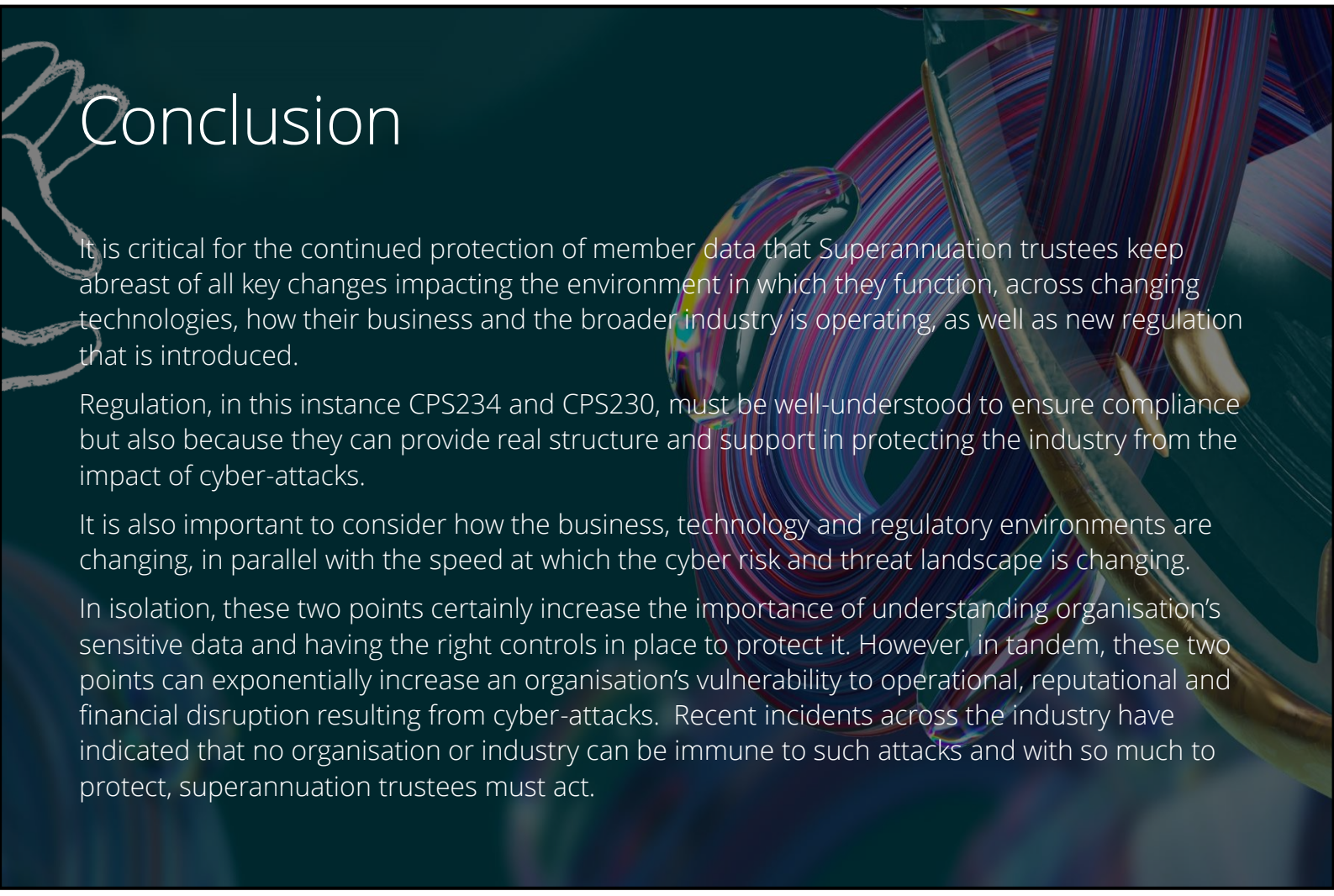
These can help reduce the number of successful phishing attempts. Doing so will in turn protect members' best financial interests.

Successful phishing attacks can open companies up to other, more serious attacks, such as ransomware. Lessons learnt from institutions recovering from ransomware attacks include:

- Maintaining data and system configuration backups
- Encrypting data

Additional measures to prevent ransomware attacks also include:





Conclusion

It is critical for the continued protection of member data that Superannuation trustees keep abreast of all key changes impacting the environment in which they function, across changing technologies, how their business and the broader industry is operating, as well as new regulation that is introduced.

Regulation, in this instance CPS234 and CPS230, must be well-understood to ensure compliance but also because they can provide real structure and support in protecting the industry from the impact of cyber-attacks.

It is also important to consider how the business, technology and regulatory environments are changing, in parallel with the speed at which the cyber risk and threat landscape is changing.

In isolation, these two points certainly increase the importance of understanding organisation's sensitive data and having the right controls in place to protect it. However, in tandem, these two points can exponentially increase an organisation's vulnerability to operational, reputational and financial disruption resulting from cyber-attacks. Recent incidents across the industry have indicated that no organisation or industry can be immune to such attacks and with so much to protect, superannuation trustees must act.

Contacts

Caroline Cui
Partner
Risk Advisory
Sydney
carolcui@deloitte.com.au

Ian Blatchford
Partner
Risk Advisory
Brisbane
iblatchford@deloitte.com.au

Neil Brown
Partner
Audit and Assurance
Melbourne
nbrown@deloitte.com.au

Contributed By:

- Ally Macleod: Partner – Accounting and Internal Controls, Risk Advisory
- Caroline Brell: Partner – Regulatory and Legal Support, Risk Advisory
- Caroline Cui: Partner – Cyber and Strategic Risk, Risk Advisory
- Dave Owen: Partner – Cyber and Strategic Risk, Risk Advisory
- Emma Trenear: Graduate – Cyber and Strategic Risk, Risk Advisory
- Eric Leo: Director – Quality Risk and Regulatory, Enabling Areas
- Georgia Hackett: Senior Analyst – Cyber and Strategic Risk, Risk Advisory
- Melissa Gomes: Partner – Regulatory and Legal Support, Risk Advisory
- Muhammad Inam Ul Huq: Specialist Director – Cyber and Strategic Risk, Risk Advisory
- Sean Moore: Partner – Regulatory and Legal Support, Risk Advisory

Endnotes

https://www.apra.gov.au/news-and-publications/apra-releases-superannuation-statistics-for-september-2022

https://www.smh.com.au/business/banking-and-finance/why-top-super-funds-are-taking-admin-in-house-20201030-p56a6v.html

https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf

https://www.afp.gov.au/news-media/media-releases/online-fraud-syndicate-dismantled-after-allegedly-siphoning-millions

Deloitte.