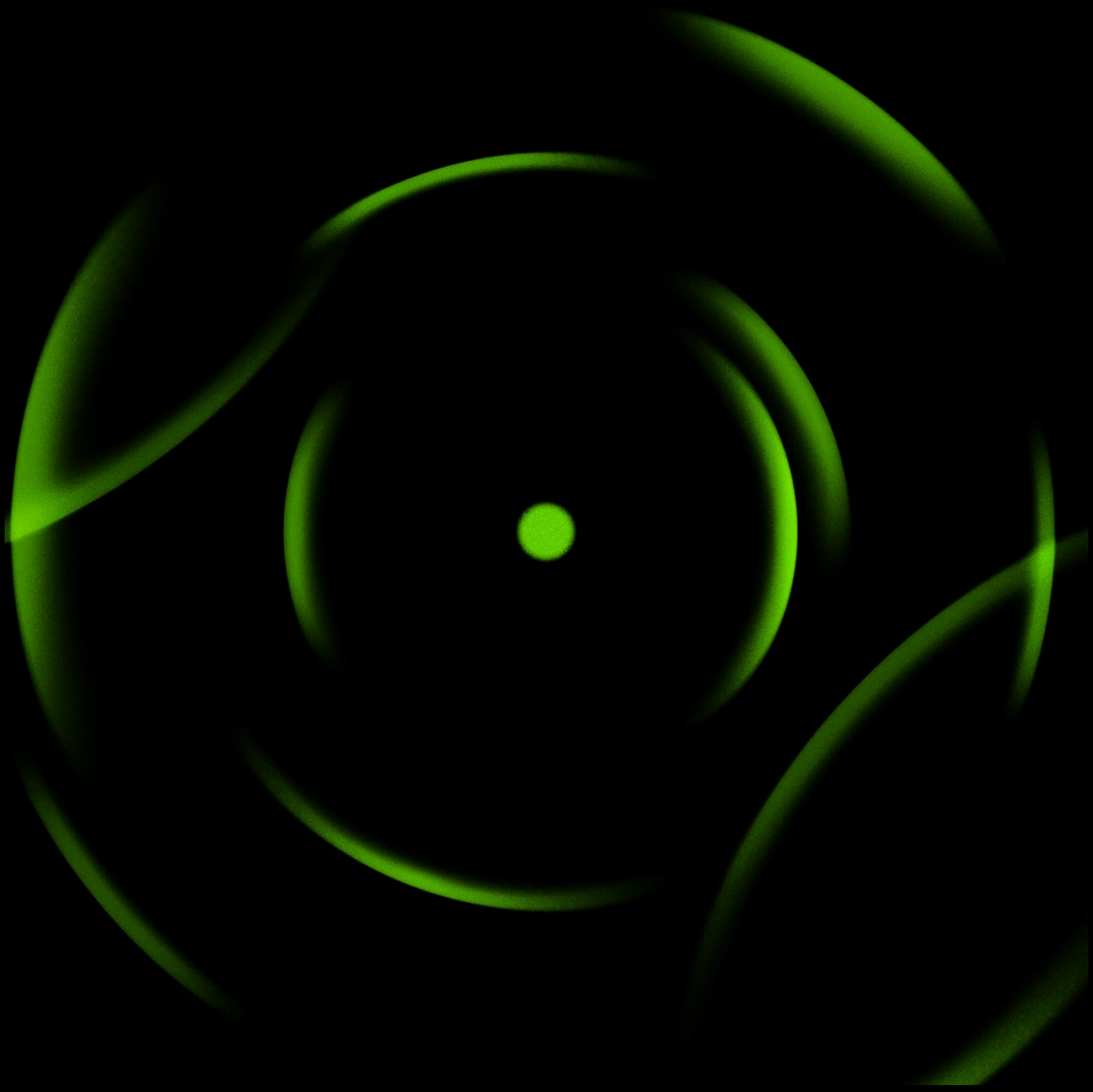
Deloitte.



Cyber Resilience: A Competitive Advantage for Australia's Superannuation Industry

Board and executive briefing paper

May 2025

Addressing recent cyber attacks on the super industry

Cyber-attacks reported in April 2025 targeting Australian superannuation funds reinforce the reality that threat actors see the sector as attractive. However, it also acts as a reminder of the opportunity to drive strategic advantage through member trust and elevated digital experience.

Attacks against multiple funds

In April 2025, news broke of coordinated cyberattacks across several super funds, affecting thousands of members. While the funds responded quickly to secure accounts, the incident resulted in member impacts ranging from unauthorised financial withdrawals through to anxiety due to uncertainty as to whether they had been targeted.

The primary attack entry point is understood to have been credential stuffing, a common cyberattack technique exploiting compromised usernames and passwords from previous data breaches unrelated to the funds. This was followed by deliberate attempts to change personal details such as telephone numbers and bank information before withdrawing funds.

In the aftermath, there was diversity in communication strategies – whether media statements were made, timing of direct member communication, and channels used.

Maturity of super's cyber posture

Following the attack, various commentators pointed to the super industry's perceived lower cybersecurity posture compared with other parts of the financial system.

There are opportunities for funds to continue their investment in defences such as MFA, and extend into newer capabilities such as phish-resistant passwordless / passkey authentication, which are beginning to become more prevalent in other industries.

There is also a trend beyond user authentication (traditional checks based on password credentials) towards enhanced identity verification at key transaction points to make sure that a person really is who they appear to be.

Safeguarding the nation's prosperity

Australia's superannuation system stands as one of our greatest national achievements – over $4 trillion in retirement savings that secure the future prosperity of millions. This immense pool of wealth embodies the financial security and dignity in retirement that Australians have worked their entire lives to build.

In this digital age, cybersecurity has emerged not merely as a defensive necessity but as a strategic enabler that can transform member experiences and create genuine competitive advantage.

Digital transformation with digital trust

The super industry is in the midst of a profound digital evolution. Historically operating through institutional relationships, funds are developing direct-to-member digital experiences. This deepens member relationships but requires a fundamentally different approach to security.

Forward-thinking funds are applying security as a catalyst for innovation rather than viewing it as a constraint or compliance requirement. By integrating security from design stage, they discover that robust protections and exceptional user experience can be complementary rather than contradictory goals.

Trust has always been the foundation of financial services, but in today's environment, it must be continuously earned through transparent actions and effective protection. Research consistently shows that members will accept additional security steps when they understand the purpose and value these measures provide.

What is credential stuffing?

Credential stuffing is a cyberattack where hackers attempt to login using stolen usernames and passwords to gain unauthorised access to online accounts.

This attack takes advantage of the common habit of reusing passwords across multiple websites. If someone's credentials are compromised in a data breach (e.g., from social media, retail sites, or other platforms), attackers can test those credentials against accounts on other websites, including superannuation portals. Because many users repeat passwords, credential stuffing attacks can be highly effective.

Driving advantage through cyber resilience

For super funds to generate competitive advantage through their cybersecurity capability, we recommend focusing on five areas.

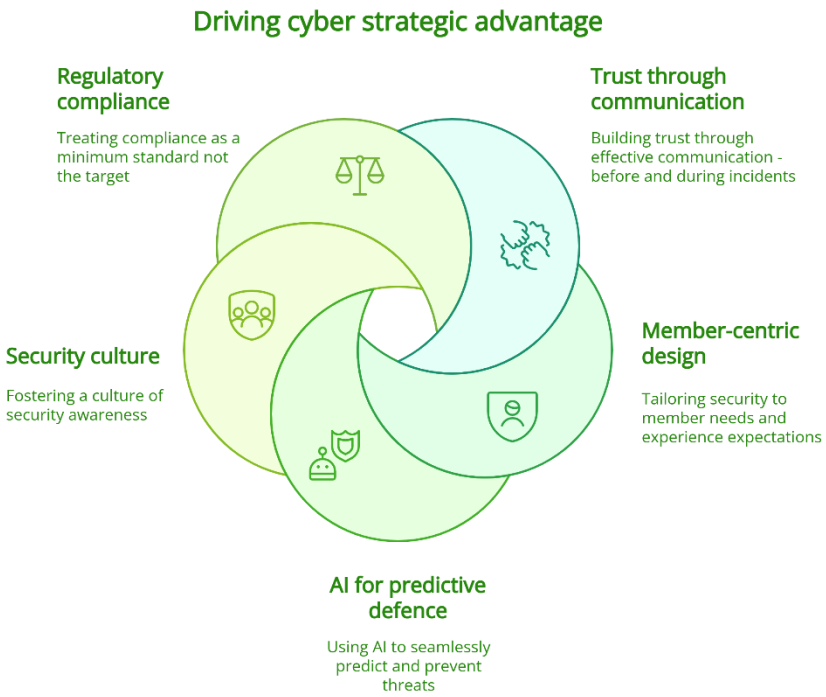
Enhance trust through communication

By clearly communicating how security controls protect member assets, funds transform what could be perceived as friction into a trust-building interaction. For instance, when implementing multi-factor authentication, messaging that frames this as "additional protection for your retirement savings" resonates more effectively than technical explanations about security protocols.

The most successful funds have moved beyond fear-based security messaging to adopt a more positive approach grounded in nudge theory. Rather than alarming members about potential threats, these communications emphasise the proactive protections in place and the fund's commitment to safeguarding retirement futures. This positive tone aligns security with member well-being rather than as an obstacle to overcome.

And when, despite all the fund's efforts, an incident does occur, rapid transparent communication is key so that members are not left in the dark and trust can be eroded in the vacuum of information. Conversely, proactive and effective engagement with members in a crisis can even build trust despite the unfavourable circumstances.

In our view, leading funds use all channels of member communications, not just traditional methods, and extend that to all members rather than just those impacted. They also communicate when an event affects others (but not them), further reinforcing trust. And before using these channels, they prove and test them for resilience and rapid response.



Design security with members at the heart

The superannuation member base spans multiple generations, each with different digital expectations and security awareness. Rather than implementing one-size-fits-all solutions, leading financial services organisations design security experiences tailored to diverse member segments.

For digitally confident members, this might involve streamlined authentication with biometric options and minimal interruptions. For less tech-savvy members, it could include additional guidance, clearer explanations, and alternative verification pathways.

The key insight is that security controls can be personalised without compromising protection, creating experiences that respect member preferences while maintaining robust safeguards.

This personalised approach extends to cyber awareness strategies as well. Effective security education must resonate with the specific concerns and digital comfort levels of different member segments.

Younger members may respond to gamified security awareness, while older members might prefer more traditional educational formats. By meeting members where they are, funds transform security education from a checkbox into a valuable member service.

Embed Artificial Intelligence (AI) for predictive defence

AI offers a transformative technology for superannuation security, amplifying rather than replacing human capabilities. Within the next 12-18 months, we will see AI embedded throughout member journeys, silently analysing patterns to identify potential threats while remaining virtually invisible to legitimate users.

Imagine a member changing their bank account details – a routine transaction that could also indicate potential fraud. Advanced AI systems can evaluate dozens of contextual factors within milliseconds: Is this the first account change in years? Does the new account match naming conventions? Is the member accessing from a recognised device and location? Based on this analysis, the system determines whether to process the transaction immediately, or introduce additional verification beyond the existing authentication at first login.

This intelligent approach means enhanced protection for vulnerable members while maintaining frictionless experiences for routine transactions. It represents security that adapts to individual member context rather than imposing universal friction, enabling a proactive posture that builds trust.

Build security culture from within

A fund's cyber resilience ultimately depends on its people. While sophisticated technical controls remain essential, the human element continues to represent both the strongest defence and the most vulnerable attack surface. Creating a security culture where every employee understands their role in protecting member assets requires more than annual compliance training.

Progressive funds are fostering security champions across all business functions – individuals who promote secure practices and serve as bridges between technical security teams and operational staff. This distributed approach ensures security considerations become embedded in everyday decisions rather than siloed within a specialised area.

For funds that outsource their operations, this also needs to extend to the supply chain, assessing the security culture of material service providers.

When faced with sophisticated social engineering attempts, employees grounded in this positive security culture recognise their crucial role in member protection. Their vigilance does not stem from fear of punishment but from a genuine commitment to safeguarding the retirement savings entrusted to their care.

Treat regulatory compliance as the floor, not the ceiling

Australia's regulatory framework for superannuation cybersecurity provides a solid foundation through APRA's CPS 230 and 234 standards, Financial Accountability Regime (FAR) and recent ASIC enforcement. However, truly member-centric funds recognise that these requirements represent minimum expectations rather than the target.

The most security-mature organisations have moved beyond compliance-driven approaches of providing the minimum capabilities that could be justified to a regulator, and are instead orienting themselves against member expectations. They recognise their duty extends beyond legal requirements to implementing controls that members would reasonably expect for protecting their retirement savings as part of the trustee's duties.

This distinction between compliance and commitment manifests in how funds approach security investments. Rather than allocating resources based on regulatory mandates and hot topics, forward-thinking funds assess potential security initiatives based on members' best financial interests and risk reduction – ensuring investments directly enhance protection for the assets in their care.

The path forward

The time is right for boards and executives of superannuation funds to lean into enhanced member trust and experience through their cyber capabilities

Now is the time

Australian superannuation funds have reached an inflection point where cybersecurity represents a strategic opportunity rather than merely a risk management function. Those embracing this mindset will differentiate themselves through member experiences that seamlessly integrate protection with usability.

The future belongs to funds that:

- Position security as a positive enabler of member confidence rather than a necessary obstacle
- Personalise protection to respect diverse member preferences and digital comfort levels
- Leverage AI and automation while maintaining human judgment where it matters most
- Foster security cultures where protection becomes everyone's responsibility
- Exceed compliance requirements based on commitment to member protection

In an environment where digital trust has become the new currency, these approaches do not just protect Australia's retirement savings – they create genuine competitive advantage through member experiences built on confidence and security. The question for fund boards and executives is not whether cybersecurity matters or if they are compliant, but whether they are harnessing its full potential as a strategic enabler for member value in an increasingly digital future.

Measuring what matters

Boards and executives do increasingly recognise cybersecurity as a strategic priority, but many struggle to identify meaningful metrics amid technical complexity. While perspectives vary across management teams, several key indicators have emerged that provide valuable insights into security program effectiveness:

- **Member trust** indicators measure confidence in the fund's security practices
- **Security experience** scores track how protection mechanisms affect the member journey
- **Threat detection efficiency** captures how quickly potential compromises are identified
- **Response capability** metrics evaluate the organisation's ability to contain threats

The most valuable measurements track trends over time rather than focusing on absolute values. Improvement trajectories often reveal more about security program effectiveness than point-in-time assessments, especially in an environment where threats continuously evolve.

Contacts

Kate Monckton
Cyber Strategy & Transformation Leader
kmonckton@deloitte.com.au

Evan Carvouni
Cyber Defence & Resilience Leader
ecarvouni@deloitte.com.au

Fiona O'Keefe
Superannuation Partner, Audit & Assurance
fiokeefe@deloitte.com.au

Jarrod Oakley
Digital Trust & Privacy Leader
jaoakley@deloitte.com.au

Tim Worner
Superannuation Wealth and Advisory Leader
tworner@deloitte.com.au

Mel Gomes
Superannuation Partner, Risk & Regulation
melgomes@deloitte.com.au

Andrew Boal
Partner, Actuarial Consulting
aboal@deloitte.com.au

Steve Freeborn
Partner, Actuarial Consulting
stfreeborn@deloitte.com.au