**Ben Di Marco, Willis Towers Watson**

Cyber Specialist

**Theresa Lewin, Willis Towers Watson**

Financial Institution Leader

**Lucy Cooper, Willis Towers Watson**

Senior Consultant

# Unpacking CPS 234 Information Security

## What it means for superannuation fund trustees

Ben Di Marco, Theresa Lewin and Lucy Cooper

A complex web of cyber security obligations has been created for the superannuation industry with the advent of a recent prudential standard in regard to information security. Many funds are struggling to develop strategies to address what is now required.

APRA's cross-industry *Prudential Standard 234 Information Security* (CPS 234) applies to, among others, all RSE (Registrable Superannuation Entities) licensees under the *Superannuation Industry (Supervision) Act 1993*.

The standard commenced on 1 July 2019, and all information assets managed by third parties must comply with CPS 234 by the earlier of 1 July 2020, or the date when an information technology provider's contact is renewed. So, what are some practical measures that funds and trustees can take to ensure compliance with CPS 234?

### What is CPS 234?

Introduced to ensure that APRA-regulated entities adopted appropriate resiliency measures against security incidents (including cyber-attacks), CPS 234 requires such organisations to maintain an information security capability commensurate with their profile, relevant vulnerabilities and likely threats. Entities must also have the capability to respond swiftly and effectively in the event of a data breach. The standard builds on APRA's recent work in cloud outsourcing practices, *Prudential Standard CPS 231 Outsourcing* and *CPS 232 Business Continuity*.

CPS 234 adopts a risk principle approach to cyber security and goes beyond box-ticking compliance approaches. The standard provides that the board of an APRA-regulated entity is ultimately responsible for that entity's information security capability; for superannuation funds, this means the trustee directors. CPS 234 requires trustees to implement cyber risk identification practices and develop an information security capability that manages the size and extent of likely information assets threats.

The standard contains onerous incident reporting obligations, and trustees must notify APRA as soon as possible and within 72 hours of experiencing an information security incident that 'materially affects or has the potential to materially affect' the entity or members or has been notified to other regulators. They must also notify APRA within 10 business days after becoming aware of a material information security control weakness that cannot be remediated in a timely manner.

## Other trustee obligations

CPS 234 also requires entities to:

- clearly define information security roles and responsibilities of the board, senior management, governing bodies and individuals
- assess the information security capability and controls of any third party that manages information assets
- implement controls to protect information assets and undertake regular testing and assurance of the effectiveness of controls
- enhance information security capabilities to respond to any changes in potential vulnerabilities, threats, information assets or the business environment
- maintain an information security policy framework
- develop robust mechanisms to detect and respond to information security events in a timely manner.

While only APRA-regulated entities must comply with the standard, its requirements apply to all its 'information assets', whether managed by the entity itself, third parties or related entities.

## Third-party processors and the cyber risk supply chain

Under the standard, internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties. These requirements reflect APRA's communicated view that cyber risk ownership rests within the organisation and cannot be outsourced.

Trustee directors have onerous obligations to monitor the information security capabilities of outsourced service providers. They must satisfy themselves that the service provider's systems meet the entity's CPS 234 obligations. Service providers must also be capable of meeting APRA's requirements to notify information security incidents within 72 hours of becoming aware of an event which may materially affect the entity or its members.

The standard creates supply chain obligations and can attach to the systems and controls of any third party who has access to the organisation's information assets. This means the capabilities of a managed service provider's own suppliers and partners can create compliance risk and that, for critical systems, the entire information security supply chain may be relevant.

## Compliance, insurance and risk mitigation

APRA's Executive Board Member Geoff Summerhayes gave insights into the regulator's priorities for CPS 234 at last year's CyBSA 2019 Breach Simulation Event.

In a keynote speech, Mr Summerhayes highlighted that APRA licensees could not 'secure what [they] don't understand' and that their defences were only as strong as their supply chain's 'weakest link'. He stressed that compliance with the standard must address each organisation's individual circumstances and provide assurance around the organisation's security capability and ability to minimise the impact of any compromise.

Mr Summerhayes' comments reflect the standard's focus on entities examining their systems risk and understanding what financial and other harms can result for the fund and its members. For these reasons, CPS 234 compliance frameworks should be supported by a strong foundation of enterprise-wide risk assessments and effective identification of key data assets, and common points of exposure.

Comprehensive cyber insurance is also a critical support when managing a cyber crisis and can mitigate the financial loss of a cyber event. Trustees examining CPS 234 should test whether they hold comprehensive cyber insurance and if it is integrated into the organisation's incident response plan and stakeholder protection capability.

Trustees must also maintain high visibility over CPS 234 programs as they are held ultimately responsible for ensuring that the entity has appropriate information security investments in place.

## Cyber risk and organisational culture

Numerous Australian regulators have recognised that cyber resilience requires a culture that promotes the right behaviours and mindset among employees. This requires regularly monitoring the strength of the culture and then developing organisation-wide programs that address identified gaps, build awareness and drive the desired employee behaviours.

Trustees need to be alive to potential cultural risks—research undertaken by Willis Towers Watson and ESI Thought Lab found nine out of ten organisations consider untrained or negligent staff is their greatest cyber risk, and nearly 65% of all reported cyber claims result from a human element failure. By driving the right behaviours, organisational culture is, therefore, an important line of defence for organisations and a key input for meeting CPS 234 requirements.

Fostering the right culture requires trustees and leaders to be accountable for the organisation's culture by monitoring the health of the culture on an ongoing basis and ensuring processes are in place to address hotspots and effect positive behavioural changes. Culture should, therefore, be a key input into the accountability principles that underpin CPS 234. **FS**

**The quote**

*The standard provides that the board of an APRA-regulated entity is ultimately responsible for that entity's information security capability.*