The Role of Boards in Building Cyber Resilience

Cyber resilience insights from APRA’s recent pilots for regulated organisations have highlighted the need for boards to drastically improve their oversight of information security.

Cyber resilience is all about how your organisation continues to operate critical business functions when cyber security and operational controls start to fail. But it is the board’s responsibility to ensure that controls are implemented to protect information assets commensurate with the criticality and sensitivity of those assets and undertake systematic testing and assurance regarding the effectiveness of these controls. APRA recently reported they are failing miserably.

Just over a year ago we published an insight “Are You Ready for APRA’s CPS 234 Tripartite Assessment” (https://www.tannhauser.com.au/insights/cps234ap). Here we discussed the requirement for all APRA related entities to ensure that their information security capabilities (resources, skills and controls) were commensurate and proportionate to the size and extent of the threats to their business. In addition, we advised that APRA had reported that many entities who were assessed against the requirements of CPS 234 were found to be non-compliant in the following areas:

- Testing programs;
- Control environments; and
- Incident response capabilities.

Fast forward 12 months, and APRA has recently completed two pilot initiatives as part of APRA’s 2020-2024 Cyber Security Strategy which included among other things an independent assessment of an entity’s compliance with CPS 234, and a review of data collection to help APRA identify sources of potential cyber control weaknesses.

This latest APRA Insight on the subject points the finger squarely at boards and concluded that they need to take a more active role in challenging management of information provided on cyber resilience, ensuring how well their organisation can recover for an attack, and drill down into third party risk and the effectiveness of security controls across the supply chain. This identifies a number of recommendations on how boards can take more ownership of the risks associated with cyber security.

How does Tannhauser assist your business in addressing CPS 234?

Cyber Resilience: We help you develop incident response management plans, train staff how to respond to a cyber attack and effectively test these in real-time with simulation workshops and red team exercises.

vCISO (Virtual Chief Executive Officer): Reviewing and challenging information reported to the board by management on cyber resilience is critical in ensuring you are meeting your fiduciary duty. Tannhauser can help by working directly with the board on an ad hoc basis consulting, reviewing, and coaching the board on cyber resilience.

Cyber Risk Assessment: We perform or evaluate your cyber risk assessment in defining both the criticality and sensitivity of your information assets, as well as the size and extent of the threats faced. This includes gap analysis of existing security controls against the standard, and ALSO your exposure to third-party service providers in your supply chain.

Internal Audit Staff Augmentation: We appreciate companies will have a challenge resourcing staff adequately to perform the internal audit requirements. Cyber security expertise may be lacking in Internal Audit teams. Our Tannhauser team will augment your existing internal audit function capability.

Independent Testing: We perform independent security control audit and testing for a variety of complex technology environments. This includes testing relevant information security controls where information assets are controlled by a managed service provider, based on the criticality and the threat to the information assets.

Contact us for the latest cyber security updates to regulatory and legislative requirements for your business.

Further APRA Prudential Standard CPS 234 Information Security guidance is located here: