SQUIRE PATTON BOGGS

What Does APRA's Proposed Standard for Information Security Management Mean for Your Business?

With new data breach notification laws having come into effect in February 2018 and APRA releasing its draft standard for Australian Prudential Regulation Authority (**APRA**) regulated entities, aimed at tackling the threat of cyberattacks, it is inevitable that APRA regulated entities and perhaps other entities which suffer information security attacks, including government agencies, will be the subject of legal claims, including class actions.

On 22 February 2018, the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) came into force, requiring government agencies and businesses subject to the Privacy Act 1988 (Cth) to notify any individuals affected by a data breach that is likely to result in serious harm. The Office of the Australian Information Commissioner must also be notified of such data breaches (see our previous article on the notifiable data breaches scheme).

On 7 March 2018, APRA released draft prudential standard: CPS 234 Information Security (CPS 234) and a discussion paper: "Information Security Management: A new cross-industry prudential standard". APRA's media release states that CPS 234 is "aimed at shoring up the ability of APRA-regulated entities to repel cyber adversaries or respond swiftly and effectively in the event of a breach." APRA is seeking submissions regarding CPS 234 in March 2018.

In summary, proposed new standard CPS 234 requires regulated entities to:

- Clearly define information security-related roles and responsibilities of the board, senior management, governing bodies and individuals
- Maintain information security capability commensurate with the size and extent of threats to information assets, and which enables the continued sound operation of the entity
- Implement information security controls to protect its information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls
- Have robust mechanisms in place to detect and respond to information security incidents in a timely manner
- Notify APRA of material information security incidents

CPS 234 (or some form of it) will likely form the standard which APRA regulated entities will be required to meet with respect to information security. That standard may by extension also be relevant to non-APRA regulated corporates and government entities which collect information the disclosure of which may results in serious harm. APRA's discussion paper highlights that an entity's board and senior management are ultimately responsible for information security. This is apparently based upon an observed gap in board engagement on this topic.

Satisfying the requirements of proposed CPS 234 may reduce the risk of an information security attack or limit the damage it causes. However, in the event of such an attack on an APRA regulated entity, and perhaps any large entity, that entity, its board members and senior management may nevertheless face legal claims from both customers and shareholders, including class actions. As noted in our note concerning the new privacy legislation, in the US, increased visibility of data breaches has inevitably resulted in such claims.

Claims may be brought by individuals, or more likely classes of individuals, who have suffered a loss as a result of the attack as well as shareholders where the attack causes a significant drop in the entity's share price or the entity fails altogether. In the face of such a claim, it will be important that the entity, its board and senior management are able to establish that they have at least met the requirements of CPS 234.

With the threat of material loss as a result of a cyber-incident being seen as inevitable, it is crucial that corporates, their boards and senior management ensure that they have well developed and appropriate cybersecurity policies and procedures in place. If you would like us to assist you in preparing such policies and procedures or a submission to APRA concerning draft CPS 234, please let us know.

Contacts

Amanda Banton
Partner
T +61 2 8248 7850
E amanda.banton@squirepb.com

Susan Goodman
Of Counsel
T +61 2 8248 7873
E susan.goodman@squirepb.com