Senate Economics Legislation Committee

ANSWERS TO QUESTIONS ON NOTICE

Treasury Portfolio

Supplementary Budget Estimates

2016 - 2017

Department/Agency: Australian Prudential Regulation Authority
Question: 175
Topic: Cyber security
Reference: Written
Senator: Ketter, Chris

Question:

1. What is APRA's role vis-à-vis cyber-attacks on financial institutions?
2. APRA has made public concerns regarding the cyber security with regards to superannuation funds. What risks do attacks of this nature pose?
3. APRA has indicated that it "intends to lift the supervisory and regulatory expectations for regulated entities to not only secure themselves against cyber-attacks, but to implement improved mechanisms to quickly identify and remediate successful attacks when they occur". What actions are APRA considering in this space?

Answer:

1. The role of APRA is developing and enforcing a robust prudential framework that promotes prudent behaviour by ADIs, insurance companies, superannuation funds and other financial institutions it supervises, with the key aim of protecting the interests of their depositors, policyholders and superannuation fund members. To this end, APRA seeks to assess the adequacy of regulated entities' preparation for managing and recovering from risks including those for cyber attacks. Institutions should seek to ensure an adverse security event does not have the potential to compromise its ability to meet financial promises, fulfil service obligations, and manage risks. In this case, preparedness includes appropriate ongoing investment in tested prevention, detection and response capabilities for managing this risk.

2. Cyber-attacks is broad term that refers to the use of computer-based technology to compromise confidentiality, integrity or availability of IT assets. These attacks can involve both external and internal perpetrators seeking financial gain (e.g. theft, fraud, extortion) or other objectives such as notoriety or political/social change.

   APRA undertook a survey between October 2015 and March 2016 to gather information on cyber security incidents and their management within APRA-regulated sectors. Superannuation industry respondents reported a higher occurrence of incidents as compared to other industries. Possible explanations are that the superannuation industry is a more attractive target to perpetrators due to the relatively high customer account balances, and/or variances in reporting thresholds between the industries.

3. APRA is developing a prudential standard on security to set requirements in place of current guidance on good practice. In this area, good practice includes an emphasis on timely detection and response to security compromises, and regular testing of response plans.

APRA also plans to repeat the cyber security survey every 12-18 months to allow APRA to monitor changes in industry and identify trends and potential issues which require a regulatory response.

Additionally, APRA has increased emphasis on cyber security as part of normal supervisory activities. In particular, assessment of areas such as governance & oversight, strategy & funding, incident detection & response (i.e. not just prevention), capabilities & resourcing and situational awareness & collaboration.