CYBER RESILIENCE FOR FINANCIAL SERVICES ENTITIES

Date: 20 May 2015

Australia Investment Management Alert

By: Jim Bulling, Julia Baldi

ASIC REPORT 429

In March this year, the Australian Securities and Investments Commission (ASIC), issued Report 429 Cyber resilience: Health check (REP 429). The report aims to highlight the importance of cyber resilience for entities regulated by ASIC, including Australian Financial Services Licence holders, Australian Credit Licence holders and listed entities. The Report indicates that ASIC is keen to ensure that Australia keeps pace with developments in Europe and the United States in combatting cybersecurity risks.

REP 429 is based on existing law and sets out the measures which ASIC believes regulated entities should already have implemented, in order to meet their compliance obligations relating to privacy of stored data and cybersecurity generally. REP 429 notes that for entities regulated by the Australian Prudential Regulation Authority (APRA), risk management and resource requirements are set and enforced by APRA, not ASIC.

However, the principles discussed in REP 429, put APRA regulated entities on notice of the types of risk management and governance issues which arise in a cybersecurity context. We also note that from 1 July 2015 superannuation dual-regulated entities that are both a responsible entity of a registered managed investment scheme and a registrable superannuation entity licensee will be regulated by both APRA and ASIC for their risk management and resource requirements.

Health Check

In order to assist regulated entities in determining whether their cyber risk management practices are adequate, ASIC has identified a set of 'cyber health check prompts'. At a high level, the prompts encourage entities to address questions such as:

- whether the entity's board and senior management are aware of cyber risks, and the extent to which management has oversight of legal and compliance obligations in relation to cyber security
- whether the entity has assessed what information and business assets are essential to the operation of the business, and how such operational assets are protected and valued
- whether the entity is exposed to cyber risk from third party providers, and how such risks may be minimised
- the extent to which cybersecurity forms part of the risk management procedures of the entity and the level of awareness of cyber risk in the business generally

- whether the entity has effective detection, response and recovery systems in place in the event of a cyber attack

National Institute of Standards and Technology Framework

In addressing measures which entities may undertake to improve their cyber resilience, ASIC has indicated that the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Framework) has particular relevance for its regulated population. The NIST Cybersecurity Framework was initially developed by the U.S. National Institute of Standards and Technology (an agency of the United States Department of Commerce) for U.S. government entities dealing with sensitive information and has since been widely adopted by U.S. financial institutions and other entities dealing with sensitive information.

The Framework sets out the core functions of cyber resilience procedures.

a) Identify:
Entities should identify their most critical intellectual property, assets and stored data. In addition, entities should seek to develop institutional understanding of their cybersecurity risks and potential areas of exposure to cyber risks within the business. This should include an assessment of the business' governance and oversight policies and procedures and of ongoing risk management tools, as well as a review of the entity's business environment and associated risks.

b) Protect:
Entities should develop and implement procedures and safeguards to protect their critical assets. This will typically include controlling access to critical assets through identification protection features, implementing mechanisms to increase awareness and training on cyber risks for staff, mandatory cyber security obligations for third party providers, as well as having in place protective technology such as encryption services and secure networks.

c) Detect:
Entities should put in place technology, procedures and resources to detect a cybersecurity breach. Entities should aim to have in place a baseline of normal operations so that anomalies may be detected (for instance a spike in online posting or financial activity), to implement continuous monitoring of cybersecurity (for example to identify malicious codes) and to stress test and maintain these protections to ensure detection is working effectively.

d) Respond:
Entities should put in place technology, procedures and resources to respond to a cybersecurity breach. A response plan should be developed which addresses the roles of internal and external stakeholders, communication to effected persons, how events may be contained or mitigated and an analysis of methodology to determine the extent of the breach and how it occurred.

e) Recover:
A recovery plan should be put in place, that ensures timely reinstatement of systems and identification of improvements and lessons learned in the event of a breach.

Reporting Cyber Breaches

As well as pointing to relevant overseas developments, REP 429 outlines a number of cyber resilience resources available in Australia.

In particular, ASIC highlights the Australian Government initiative ACORN, an online system that allows the public to securely report instances of cybercrime, as the appropriate reporting forum for small to medium-sized businesses, while large businesses should report to Australian Cyber Security Centre (ACSC) the Australian Government's cybersecurity law enforcement, defence and security agency.

ASIC also recommends a number of Australian providers who deal with mitigating cyber risk including the Australian Signals Directorate (ASD) publication *'Strategies to mitigate targeted cyber intrusions*' and CERT Australia, who partner with major Australian businesses, particularly major financial institutions and market infrastructure providers in providing advice and support on cyber risks.

OTHER CYBERSECURITY DEVELOPMENTS

In March 2015 the UK Government issued a report on cybersecurity insurance which details new joint initiatives between Government and the insurance sector to help organisations address their cybersecurity risks. The report suggests that organisations seek to obtain "Cyber Essentials Certifications" from insurers to demonstrate that they have adequate cybersecurity insurance in place. Such insurance is becoming increasingly relevant when considering that the growth in the level of cyber attacks on Australian businesses was estimated at 20% during 2014.

In April 2015 the Securities Exchange Commission (SEC) Division of Investment Management published a Guidance Update which outlines measures which managed funds and investment advisers may wish to consider in addressing cybersecurity risks. The guidance includes practical tips which would also be applicable to Australian managers. You can view the Guidance Update here.

FURTHER INFORMATION

K&L Gates' financial services practice has significant experience dealing with ASIC and APRA-regulated entities in relation to the whole spectrum of risk management and prudential issues.

In addition, our IT and outsourcing practice both here and overseas has had extensive experience dealing with the technological challenges of implementing robust cybersecurity measures within large and small organisations.

If you would like more information about how your organisation should be responding to the practical and regulatory developments for financial services entities in Cybersecurity contact Jim Bulling at jim.bulling@klgates.com +61.3.9640.4383, or your K&L Gates relationship partner.

KEY CONTACTS

JIM BULLING
PARTNER
MELBOURNE
+61.3.9640.4338
JIM.BULLING@KLGATES.COM

JULIA BALDI
SENIOR ASSOCIATE
MELBOURNE
+61.3.9640.4212
JULIA.BALDI@KLGATES.COM

