MARSH

March 2015

CLIENT ALERT

ASIC REPORT 429 CYBER RESILIENCE: HEALTH CHECK

REASSESSING YOUR APPROACH TO CYBER RISK

ASIC released Report 429, *Cyber Resilience: Health Check*, on 19 March 2015, urging Australian businesses to strengthen their strategy and controls against cyber risk as the threat continues to evolve. Noting that cyber attacks affected 5 million Australians in 2013 at an estimated cost of $1.06 billion, the report offers a series of health check prompts, designed to help organisations increase their awareness of cyber risks and identify opportunities to improve their cyber resilience.

Cyber risk resilience has been earmarked by ASIC as a high risk area that will be considered in the regulator's surveillance programs in the future.

Whilst those entities regulated by ASIC have legal and compliance obligations that may require a review and update of cyber risk management practices, all businesses are encouraged to be aware of cyber risks and take action to improve cyber resilience, thus collectively improving cyber resiliency in Australia. The purpose of this alert is to highlight the key recommendations from the ASIC report and outline corporate governance obligations.

CYBER RESILIENCE

Generally speaking, cyber resilience is the ability to prepare for, respond to and recover from a cyber attack, as well as the ability to continue operating during the attack and to adapt and recover from it.

Specific to ASIC Report 429, cyber resilience is the intended outcome of cyber risk management and cybersecurity measures.

CYBER ATTACK TERMINOLOGY

The term "cyber attack" can be ambiguous as commonly used. As used within the context of Report 429, ASIC clarifies cyber attack is "...an attempted or actual incident that either:

a. Uses computer technology or networks to commit or facilitate the commission of traditional crimes, such as fraud and forgery- for example, identity or data theft (computer assisted); or

b. Is directed at computers and computer systems or other information communication technologies – for example, hacking or denial of services (computer integrity)."

PRIVACY OBLIGATIONS

The report draws a link between cyber resilience and privacy obligations that are designed to protect personal information from misuse or loss. This is noteworthy and suggests that a cyber attack compromising personal information could result in the involvement of multiple regulators.

CYBER RISK MANAGEMENT FRAMEWORK GUIDANCE

Businesses are encouraged to adopt the National Institute for Standards and Technology (NIST) Cybersecurity Framework to improve cyber risk management. The benefits of this framework include alignment of common language and benchmarks within Australia and globally. It offers a flexible and scalable risk-based environment that allows for integration with existing standards on global security and IT governance.

THE ROLE OF CORPORATE GOVERNANCE

The report makes the following observations specifically regarding board oversight, directors and officers and continuous disclosure guidance.

1. Board Oversight

Lack of active board involvement in managing cyber risks has been identified as a vulnerability. Board participation is recognised as an important element of a strong culture of cyber resilience.

The efficacy of the Cyber Risk Management Framework noted above is highly dependent upon governance consolidating core cybersecurity functions across the organisation, from board level to operational level.

2. Role of Directors

Directors are urged to review their board-level oversight of cyber risks and cyber resilience as part of their legal obligations and duties of managing material business risks by including cyber risks into governance and risk management practices.

3. Regulatory Requirements of a Director or Officer and Ramifications

Failing to meet obligations could result in fines, penalties, enforceable undertakings and licensing conditions. Specific to directors and officers of a company, it could result in disqualification from the role of a director or officer.

4. Continuous Disclosure

A cyber attack would be considered as market sensitive information and, as such, would fall within the continuous disclosure requirements of listed companies.

5. Insurance

Clarity is provided regarding corporate governance recommendations for a committee to oversee the insurance program given the business and insurable risks associated with the business. The report notes that existing insurance programs purchased by many companies may not adequately cover the impact of a cyber attack. It follows that oversight of the insurance program should include cyber insurance including a range of covers tailored to relevant cyber risks, such as data or privacy breach cover, media liability cover, extortion cover and network security liability cover

REPORTING AND NOTIFICATION GUIDANCE

1. Reporting of breaches to ASIC

Inadequacies in risk management systems may amount to a breach of companies' obligations that must be reported to ASIC. In some instances, such inadequacies may become apparent at the time of a cyber attack, highlighting deficiencies in the risk management systems.

2. Notification to Customers or Client of a Breach of their Personal Data

Presently, there are no mandatory notification requirements in place in Australia for reporting cyber attacks or data breaches per se. However, the report stresses the importance of notifying individuals such as employees, customers or clients if there is a breach of their personal data. As noted in the preceding Privacy Obligations section, applicable obligations under privacy law would trigger in the event of a cyber attack compromising personal data.

3. Mandatory Data Breach Notification Scheme

In response to the Federal Parliament's Joint Committee on Intelligence and Security's *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill* 2014, a mandatory data breach notification scheme has been proposed in March 2015 for implementation by the end of 2015.

THIRD PARTY PROVIDERS OR CLIENTS

A robust cyber resilience profile (including awareness of privacy obligations) extends to the risk management and cyber resilience of third party providers such as business partners, service providers, contractors and suppliers, customers, clients and others in your supply chain.

Forensic investigations of a well-publicised and large-scale cyber attack concluded that the 'weak link' was a third party contractor's network.

INSURANCE

ASIC notes that cyber insurance was developed to specifically target cyber exposures and, depending on an organisation's risk profile, should be considered as an appropriate business decision.

NEXT STEPS

ASIC notes that it is not possible for businesses to protect themselves against every cyber risk, however it is important that businesses are aware of the risks they may face.

For further guidance on ASIC's *Cyber Resilience: Health Check report*, or more information about preparing for cyber risks, please contact:

Susan Elias
National Manager – Cyber, FINPRO Practice
+61 7 3115 4532
susan.elias@marsh.com