Article

Cybersecurity Requirements for Licensees

Authors: Derek Stenson, Partner | **Philippa Gilkes,** Associate

Entities regulated under the Insurance Law will need to implement cybersecurity measures in proportion to their cyber risk profile by 27 November 2020 following the release of the Rule and Statement of Guidance on Cybersecurity for Regulated Entities (the "Guidance") by the Cayman Islands Monetary Authority (the "Authority") on 27 May 2020.

The Authority has acknowledged the benefits that technology offers but notes that a significant compromise in the use of technology could impact the ability of regulated entities to meet overall business objectives or result in significant liability and reputational damage. Accordingly, the Authority is of a view that it is important for regulated entities to ensure that robust cybersecurity measures are in place and that such licensees can appropriately identify, protect, detect, respond to and recover from such cybersecurity-related threats, incidents and breaches which is why the new Rule and Statement of Guidance has been introduced.

Management must implement a business-aligned proportionate cybersecurity program consisting of (i) a cybersecurity framework; (ii) information technology ("IT") policies and procedures; (iii) clear, documented processes for responding to, containing and recovering from cyber breaches; and (iv) a risk-management strategy which addresses all potential cybersecurity risks to which the regulated entity might be exposed based on their particular business activities and use of technology. Managerial responsibilities and controls must be clearly identified to ensure policies and procedures are maintained and followed. A Senior Officer must also be appointed to oversee the cybersecurity framework. Comprehensive training must also be endorsed by senior management and regularly reviewed and maintained by suitable personnel to ensure it takes into account the evolving nature of technology and relevant emerging risks. A regulated entity may adopt its parent company's cybersecurity framework however, the regulated entity must assess and document that an appropriate framework meeting the Authority's requirements is in place on a group wide and legal entity level.

If a regulated entity outsources its IT functions, the entity remains ultimately responsible for those functions and their cybersecurity. It Is incumbent upon the entity to ensure that their service provider is in compliance with the Authority's Rule and Guidance and that the entity has oversight and clear accountability for the outsourced functions as if it was performing the functions itself.

Managed Entities

Regulated entities such as Class B and C insurers that are fully managed by a licensed insurance manager ("Managed Entity") may rely on such insurance manager's cybersecurity framework. However, each such Managed Entity must be satisfied with the level of cybersecurity provided and will continue to be ultimately responsible for assessing the compliance of their insurance manager's cybersecurity framework with the Rule and Statement of Guidance requirements including ensuring that the cybersecurity framework is appropriate for the relevant Managed Entity's particular cybersecurity risk profile associated with their technology and emerging cybersecurity threats. The board of directors of a Managed Entity must require its insurance manager to report any relevant cybersecurity breaches and ensure there are mechanisms in place through which the Managing Entity, through its board of directors, is made aware of the services being provided by its insurance manager.

Notification Requirements

An insurance licensee must notify the Authority within 72 hours of discovering any incident which has a material impact on internal operations, or the potential to become a material incident. The definition of incident criticality should be defined by the insurance licenses in relation to its own management framework and cyber risk ratings if appropriate; however, incidents falling within one of the following scenarios must be reported to the Authority and any affected persons notified:

(a) Unauthorised dissemination of personal data;

(b) Significant operational impact to internal users that is material to customers or business operations;

(c) Extended disruptions to critical business systems or internal operations;

(d) Significant or growing number of customers impacted;

(e) Potential reputational impact to the entity or the Cayman Islands – in this case, immediate notification is required if there is a risk of premature public disclosure;

(f) Loss of card payment information, beneficial owner details or personally identifiable information; or

(g) Loss or exposure of data in violation of applicable foreign and domestic data protection and regulatory requirements.

Authors:

Derek Stenson
Partner
Derek.Stenson@conyers.com
+1 345 814 7932

Philippa Gilkes
Associate
Philippa.Gilkes@conyers.com
+1 345 814 7751

Cayman Insurance Contacts:

Rob Humphries
Counsel
rob.humphries@conyers.com
+1 345 814 7793

Paul Scrivener
Independent Consultant
paul.scrivener@conyers.com
+44 7393 932337

For further information please contact: media@conyers.com