

Alert

New Cyber Event Reporting Requirements for Bermuda's Insurance Industry

Author: Chris Garrod, Director | Cathryn Minors, Associate

Bermuda's Insurance Act 1978 has been amended to mandate the reporting of material cyber events by insurers, insurance managers and insurance intermediaries. The Insurance Amendment Act 2020, which became operative on 5 August, comes into force at a time of growing numbers of successful cyberattacks internationally and increased vulnerability due to remote working during the COVID-19 pandemic.

Cyberattacks can result in both financial and reputational damage. This amendment gives the Bermuda Monetary Authority (BMA), which has regulatory oversight of the Bermuda insurance industry, visibility of cyber events that result in a material impact to businesses registered under the Insurance Act.

What are material cyber reporting events?

A material cyber reporting event is considered to be any act that results in the unauthorized access to, disruption, or misuse of the electronic systems or information stored on such systems of a "registered person", i.e. an insurer, insurance manager or insurance intermediary (an agent, broker or insurance marketplace provider) (together, a "Registered Person"), including breach of security leading to the loss or unlawful destruction or unauthorized disclosure of or access to such systems or information, where:

- a) a cyber reporting event has the likelihood of adversely impacting policyholders or clients (e.g. any breach of personally identifiable information or any widespread outage of IT services);
- b) a Registered Person has reached a view that there is a likelihood that loss of its system availability will have an adverse impact on its insurance business (or on policyholders or clients, in the case of insurance managers and intermediaries) (for example, an outage of a system identified as critical that has resulted in a significant impact to normal operations);
- c) a Registered Person has reached a view that there is a likelihood that the integrity of its information or data has been compromised and may have an adverse impact on its insurance business (or on policyholders or clients, in the case of insurance managers and intermediaries) (for example, a system configuration or data file has been changed by a malicious attacker);
- d) a Registered Person has become aware that there is a likelihood that there has been unauthorized access to its information systems whereby such would have an adverse impact on its insurance business (or on policyholders or clients, in the case of insurance managers and intermediaries) (for example, a malicious code execution that has resulted in unauthorized access to a system or data); or
- e) an event has occurred for which notice is required to be provided to a regulatory body or government agency.

When in doubt about whether an event is reportable, Registered Persons should consult the BMA for guidance.

Reporting Timescales

If any Registered Person believes, or has reason to believe that a cyber reporting event has occurred, it must immediately notify the BMA and, within 14 calendar days of such notification, a Registered Person is expected to provide the BMA with a written report setting out all of the particulars of the cyber reporting event that are available to it.

All Registered Persons are expected to maintain logs of all cybersecurity incidents together with details of actions taken to resolve them. Incident logs should be available for inspection upon the BMA's request at any time.

The BMA wants to keep Bermuda's reputation as a leading reinsurance jurisdiction intact, and as cyber risk becomes increasingly prevalent in the insurance world, these legislative amendments show once again that Bermuda continues to adhere to prudentially sound international standards.

Authors:

Chris Garrod
Director, Insurance and Technology
chris.garrod@conyers.com
+1 441 299 4923

Cathryn Minors
Associate
cathryn.minors@conyers.com
+1 441 299 4902

This article is not intended to be a substitute for legal advice or a legal opinion. It deals in broad terms only and is intended to merely provide a brief overview and give general information.

For further information please contact: media@conyers.com