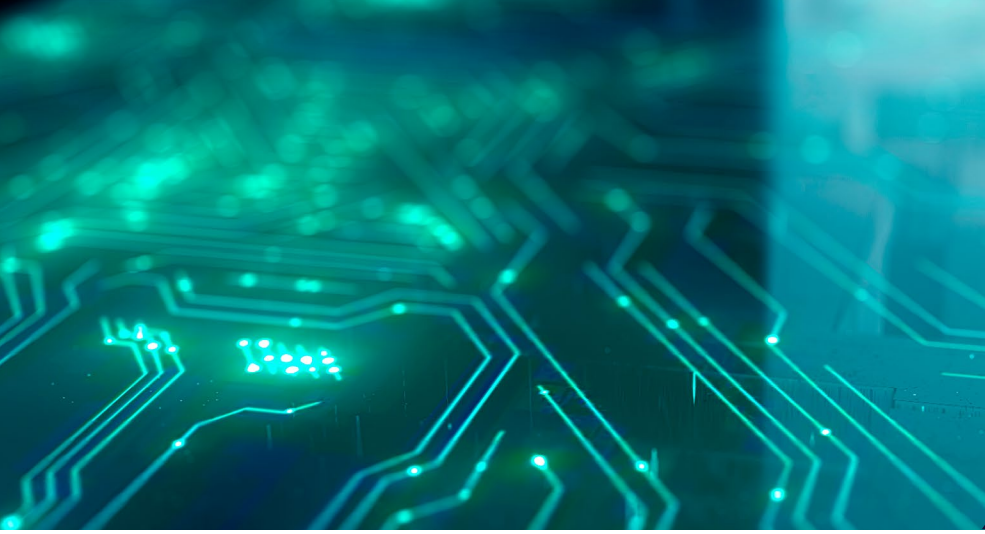

CAREY OLSEN

Cyber reporting requirements for Bermuda insurers, insurance managers and insurance intermediaries following the CrowdStrike faulty software update

Service area / Corporate

Legal jurisdiction / Bermuda

Date / July 2024

In the wake of the recent outages caused by CrowdStrike's defective software update on July 19, 2024, Bermuda insurance market participants affected by the CrowdStrike update should assess whether they need to notify their regulator, the Bermuda Monetary Authority ("**BMA**") as a result of their obligations under the Insurance Act 1978 and the Insurance Sector Cyber Risk Management Code of Conduct.

Key reporting obligations

Prompt notification

Bermuda insurers, insurance managers and insurance intermediaries (including brokers, agents and insurance marketplace providers) (each, a "**Registered Person**") must forthwith notify the BMA upon coming to the knowledge, or having a reason to believe, that a cyber reporting event has occurred. In particular, the Principal Representative (for insurers) and appropriate officer (for insurance managers and intermediaries) must notify the BMA within 72 hours from the time that there is either a determination or a confirmation of a cyber reporting event (whichever is sooner).

For these purposes, a 'cyber reporting event' is any act that results in the authorized access to, disruption, or misuse of the electronic systems or information stored on the systems of a Registered Person, including any breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to such systems or information where:

- 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);
- 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 (in the case of insurers) or clients (in the case of insurance managers and intermediaries);
- 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 (in the case of insurers) or clients (in the case of insurance managers and intermediaries);
- a Registered Person has become aware that there is a likelihood that there has been unauthorised access to its information systems whereby such would have an adverse impact on its insurance business, or on policyholders (in the case of insurers) or clients (in the case of insurance managers and intermediaries); or
- an event has occurred for which a notice is required to be provided to a regulatory body or government agency.

Only cyber reporting events resulting in significant adverse impact to the Registered Person's operations, or their policyholders or clients, must be reported to the BMA. If in doubt about whether an event should be reported, the Registered Person should consult with the BMA for guidance.

The initial report should provide a brief overview of the incident, including the nature and extent of the breach. Following the initial notification of a cyber reporting event to the BMA, the Registered Person should keep the BMA regularly updated on progress throughout the remediation of the incident.

Detailed incident report

Within 14 days of the initial notification, the Registered Person must submit a detailed incident report to the BMA setting out all of the particulars of the cyber reporting event that are available to it. This report should include:

- a comprehensive description of the cyber event;
- the date and time the incident was discovered;
- the root-cause (if this is not known then the report must still be submitted with as much information as possible);
- the systems affected;
- the potential impact on operations and clients/ policyholders; and
- actions taken to mitigate the event and prevent future occurrences.

Incident log

All Registered Persons are expected to maintain logs of all cybersecurity incidents together with details of actions taken to resolve them. Incident investigation and response logs must be kept for a minimum of five years and must be available for inspection by the BMA upon their request at any time.

Next steps

The BMA emphasizes the importance of timely and accurate reporting of cyber events. Non-compliance with these reporting obligations can result in regulatory actions, including fines, penalties or other enforcement measures.

Insurers and insurance intermediaries impacted by the CrowdStrike update should consider doing the following:

- Perform assessments to determine whether any impact from the CrowdStrike update is "material" and whether any reporting to the BMA is necessary or advisable.
- Evaluate systems, policies and practices in response to the CrowdStrike update (and other events) to identify risks and any gaps, including with respect to internal controls and disclosure controls and procedures.
- Mass IT outages highlight the importance of business continuity plans, and businesses should leverage this experience to bolster their operational resilience. Consider undertaking a review of existing business continuity plans to minimize the impact of potential future events.

If you need assistance as you and your team work through these evolving considerations or have any questions regarding this alert, please contact your Carey Olsen relationship lawyer or one of the authors listed below.

Continued

Key contacts

For further information or professional advice please contact our lawyers below:

Michelle Falcucci
Partner

D +1 441 542 4522
E michelle.falcucci@careyolsen.com

Gavin Woods
Partner

D +1 441 542 4519
E gavin.woods@careyolsen.com

FIND US

Carey Olsen Bermuda Limited
Rosebank Centre 5th Floor
11 Bermudiana Road
Pembroke HM 08
Bermuda

T +1 441 542 4500
E bermuda@careyolsen.com

FOLLOW US

Subscribe for more

Visit our corporate team at careyolsen.com

PLEASE NOTE