



## Hong Kong Insurance Authority to monitor implementation of cybersecurity guideline based on 'proportionality'

28 August 2019 | 12:05 CST

- Authority says annual cybersecurity reviews may not be sufficient
- Fitness of directors could be questioned, disciplinary action taken
- Guideline to come into effect in January

The Hong Kong Insurance Authority (HKIA) plans to monitor the implementation of a recently issued cybersecurity guideline based on "proportionality," its spokesperson told PaRR.

"The implementation of the guideline, including reviews on cyber risk mitigation, should be appropriate and commensurate with the size, nature and complexity of the business," the spokesperson said.

The HKIA's Guideline on Cybersecurity (GL20), which comes into effect in January, sets out minimum cybersecurity requirements for authorized insurers in Hong Kong – with the exception of captive and marine mutual insurance, which are self-insured.

Under Paragraph 6.2 of the GL20, insurers are now encouraged to conduct cybersecurity risk reviews on an annual basis, although the HKIA spokesperson said yearly reviews was a quoted example and may not be enough for all insurers.

Companies are not required to submit self-assessment reports to the HKIA. However, such submissions may come up for discussion when the authority begins conducting on-site visits to companies, Joyce Chan, partner with Clyde & Co told this news service.

Noting that the GL20 is principle-based, Tow Lu Lim, a partner of Mayer Brown said that until an insurer conducts an audit of what the cyber risks are, it will not know what it is facing.

Cyber risk is broadly defined in the guideline, Lim said. It includes not only external cyberattacks, but also housekeeping situations such as poor vendor management and inadequate internal controls that might result in incidents, such as disgruntled employees misusing or leaking confidential or personal data, he added.

Hong Kong has yet to enact cybersecurity legislation and data privacy matters are currently handled by the Office of the Privacy Commissioner for Personal Data, which is charged with enforcing

PROPRIETARY

**Sector:** Financial Services  
**Topics:** Cybersecurity

**Grade:** Confirmed

#### Agencies

Independent Insurance Authority (Hong Kong)  
Office Of The Privacy Commissioner For Personal Data

There are no files associated with this Intelligence

the Personal Data (Privacy) Ordinance (PDPO).

The GL20 could be seen as a supplement to the PDPO in the insurance industry to ensure information safely flows, Hannah Cassidy, partner with Herbert Smith Freehills said.

Although the guideline does not have the force of law, it has – in conjunction powers in the Insurance Ordinance (IO) – the ability to influence the HKIA's view on the continued fitness and properness of the directors or controllers of a non-complying insurer, the IA spokesperson said.

Putting the responsibility for compliance on directors will increase the likelihood that compliance with the cybersecurity guideline is properly done, according to Gareth Thomas, partner with Herbert Smith Freehills.

Lim agreed, noting that “unless the board of directors is held accountable -- with the threat that their fitness and properness is going to be put into question -- they are unlikely to make this a priority.”

The city's financial regulator – the Securities and Futures Commission – has been moving toward holding individual directors liable, too, Thomas added.

The Chief Executive of Hong Kong Competition Commission previously said targeting individuals provides a strong deterrent.

The HKIA has the power to take disciplinary actions when applicable, the IA spokesperson said.

by Joyce Chen in Hong Kong

© 2019 Mergermarket Group. All rights reserved.

To be used for the internal business of the assigned users only. Sharing, distributing or forwarding the entirety or any part of this article in any form to anyone that does not have access under your agreement is strictly prohibited and doing so violates your contract and is considered a breach of copyright. Any unauthorised recipient or distributor of this article is liable to Mergermarket for unauthorised use and copyright breach.