KPMG

Insurance Authority Guideline on Cybersecurity

Why is this important?

Hong Kong's Insurance Authority has released an industry consultation draft of the Guideline on Cybersecurity ("the Guideline") on 21 November 2018 to address cybersecurity risk, generally considered one of the top operational risks that insurers are facing. The Guideline consolidates best practices and introduces a baseline standard of cybersecurity that is expected of an authorised insurer (AI). The Guideline also echoes the Insurance Authority's recent Guideline on Enterprise Risk Management, which requires AIs to put in place cyber policies as part of their ERM framework to routinely identify, prevent, detect and mitigate cyber security threats. The Guideline will be effective by 1 July 2019, from which AIs must comply with the new requirements.

The new standards follow the trend of increasing cybersecurity regulation of the insurance industry across Asia and globally. Since 2017, bills have been introduced in China and Singapore, imposing strict security requirements to protect critical information infrastructure.

What are the focus areas?

The Guideline requires implementation of technical and non-technical measures across six focus areas, as follows:

Cybersecurity strategy and framework
A cybersecurity strategy and framework should be established, and endorsed by the Board, with reference to technology and quality assurance standards (e.g. ISO 27001, NIST framework). It should define cybersecurity objectives and the requirements for competency of people, well-defined processes and technology necessary for managing cyber risk and timely communication of the strategy with all data users. The cybersecurity strategy should be reviewed on a regular basis and upon major business/technology changes or internal/external cyber events.

Governance
The Board should hold overall responsibility for cyber security controls, including identifying responsibilities, lines of reporting and tolerance of risk. They should establish an appropriately skilled management team to be responsible for implementing measures and controls.

Identification, risk assessment and control
The management team should identify cyber threats and assess the effectiveness of measures to protect against threats. As part of the insurer's enterprise risk management program, they should put in place a self-assessment tool, which should involve mapping information assets, evaluating cyber risk and assessing impacts on the business.

Continuous monitoring
AIs should maintain a systematic monitoring process for early detection of cyber incidents. This should manage the identities and credentials of users so that any attempts to circumvent the system are clearly identified. As part of the process, all elements of the cybersecurity framework should be tested at least annually with current methodologies, for example by vulnerability assessment, scenario-based testing and penetration test.

What are the focus areas? (Cont')

Response and recovery
AIs should develop a cybersecurity incident response plan and perform incident response drills at least on a yearly basis. This should allow the insurer to restore critical functions and essential activities if a cybersecurity incident occurs. The process should include escalating the response to senior management in accordance with risk criteria defined. AIs should also report relevant incidents which have a severe and widespread impact to their operations or material impact to their services to the Insurance Authority within 72 hours.

Information sharing and training
AIs should develop a process for gathering information and sharing it with relevant groups, for example via an information intelligence sharing platform, to ensure that timely precautionary measures can be prepared against emerging threats. AIs should also promote staff professional competence and improve staff cybersecurity awareness to keep in pace with evolving cyber risks.

Assessing your readiness

The Guideline will take effect from 1 July 2019. Is your organisation ready to comply?

Key questions to assess your readiness:

- ☑ Does your cybersecurity strategy align with the business operation and environment?
- ☑ Do current risk management processes adequately highlight cyber risks for the Board?
- ☑ Does the management clearly understand the potential impact of stolen, corrupted or destroyed information assets?
- ☑ Are all elements of your cybersecurity framework tested and operating effectively?
- ☑ Are all potential scenarios accounted for in the incident response plan?
- ☑ Are you keeping up to date with and responding to the evolving cyber threat landscape?

How KPMG can help

1. Rapid diagnostic

- Perform a gap analysis of your current cybersecurity posture against the requirements set out in the Guideline

2. Formulation of cybersecurity roadmap and strategy

- Assist in developing an improvement plan to address findings identified from the gap analysis, with a roadmap detailing the expected timeline to address these gaps
- Facilitate management discussion and assist in formulating risk tolerance and appetite statement
- Integrate cybersecurity risk into the existing enterprise risk management framework

3. Cybersecurity transformation

- Provide assistance in overall project management during the implementation of the roadmap
- Assist in establishing a governance structure and management oversight process

3a. Monitoring

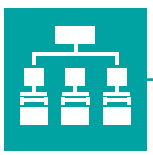
- Build up monitoring capability to detect cyber incidents
- Establish identity and access management controls for access to information assets, with the aid of automated tools
- Assist in the setup of a security operations centre internally, or with an external managed security service provider to conduct continuous monitoring
- Perform testing of all elements of the cybersecurity framework, including by vulnerability assessment, scenario-based testing and penetration test

3b. Response and recovery

- Facilitate development of a cybersecurity incident response strategy and plan to address possible incident scenarios
- Plan and execute cyber drills (practical or table-top) to test incident response capabilities

3c. Threat intelligence framework

- Establish a threat intelligence framework covering the analysis process, incident response, intelligence sharing approach, system integration approach, and the roles and responsibilities across business units



3d. Training programme management

- Deliver boardroom awareness training to improve awareness and understanding of key risks
- Assist in developing a training programme for management in order to continuously track and monitor staff development
- Assist in developing a programme to raise awareness of cyber risks

Contact us

Simon Donowho
Head of Insurance
KPMG China
T: +852 2826 7105
E: simon.donowho@kpmg.com

Henry Shek
Partner
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Bhagya Perera
Director
KPMG China
T: +852 2140 2825
E: bhagya.perera@kpmg.com

Patrick Wong
Director
KPMG China
T: +852 2140 2823
E: patrick.c.wong@kpmg.com

Brian Cheung
Associate Director
KPMG China
T: +852 2847 5026
E: brian.cheung@kpmg.com

Darryl Sim
Associate Director
KPMG China
T: +852 2847 5044
E: darryl.sim@kpmg.com

kpmg.com/cn