GL20

GUIDELINE ON CYBERSECURITY

Insurance Authority

Contents **Page**

1. Introduction

1.1 This Guideline is issued by the Insurance Authority ("IA") pursuant to section 133 of the Insurance Ordinance (Cap. 41) ("the Ordinance") and its principal function to regulate and supervise the insurance industry for the protection of existing and potential policy holders. It sets the minimum standard for cybersecurity that authorized insurers are expected to have in place and the general guiding principles which the IA uses in assessing the effectiveness of an insurer's cybersecurity framework.

1.2 Cyber risk is one of the most significant operational risks that insurers face, particularly with regard to the business operations they conduct digitally and on-line. Cybersecurity incidents can result in financial loss, business disruption, damage to reputation and other adverse consequences to an insurer. Accordingly, this Guideline requires authorized insurers to put in place resilient cybersecurity frameworks to protect their business data and the personal data of their existing or potential policyholders, and to ensure continuity of their business operations.

2. Interpretation

2.1 In this Guideline, unless the context otherwise specifies:

(a) "critical system" in relation to an authorized insurer, means a system, the failure of which will cause significant disruption to the operations of the insurer or materially impact the insurer's service to its existing or potential policy holders;

(b) "cyber risk" refers to any risks that emanate from the transmission, storage, use or processing of data transmitted, stored and retrieved in electronic means, including technology tools and platform such as computer systems, mobile applications, the internet and telecommunications networks. It encompasses data breach and leakage, loss of data, physical damage to such data caused by cybersecurity incidents, fraud committed by

misuse of and unauthorized access to data, any liability arising from data storage and transmission, and the availability, integrity, and confidentiality of such data;

(c) "cybersecurity" refers to strategies, policies, standards, practices, technology, and innovations regarding the security of an authorized insurer's systems and operations. It may encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities;

(d) "cybersecurity incident" refers to an event that threatens the security of the system of an authorized insurer which includes leakage of data in electronic form, denial of service attack, compromise of protected information systems or data assets, malicious destruction or modification of data, abuse of information systems, massive malware infection, website defacement, and malicious scripts affecting networked systems;

(e) "marine mutual insurer" means an authorized insurer which only carries on insurance business by means of its members (being owners, charterers or operators of ships or other persons related to the shipping business) mutually insuring each other against marine related risks;

(f) "relevant incident" means a system malfunction or cybersecurity incident, which has a severe and widespread impact on an authorized insurer's operations or materially impacts the insurer's service to its existing or potential policy holders;

(g) "system" means any data, hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure;

(h) "system malfunction" means a failure of any of an

authorized insurer's critical systems caused by cyber risk.

2.2 Unless otherwise specified, words and expressions used in this Guideline shall have the same meanings as given to them in the Ordinance.

3. Status of this Guideline and its application

3.1 Except for captive insurers and marine mutual insurers, this Guideline applies to all authorized insurers in relation to the insurance business they carry on in or from Hong Kong.

3.2 This Guideline should be read in conjunction with the relevant provisions of the Ordinance, other relevant Ordinances, and any other rule, regulation, code, circular and guideline made or issued under the Ordinance and other relevant Ordinances.

3.3 This Guideline does not have the force of law and should not be interpreted in a way that would override the provision of any law. A non-compliance with the provisions in this Guideline would not by itself render an authorized insurer liable to judicial or other proceedings. A non-compliance may, however, reflect on the IA's view of the continued fitness and properness of the directors or controllers of authorized insurers to which this Guideline applies. The IA may also take guidance from this Guideline in considering whether there has been an act or omission likely to be prejudicial to the interests of policy holders or potential policy holders (albeit the IA will always take account of the full context, facts and impact of any matter before it in this respect).

3.4 Whilst this Guideline seeks to assist authorized insurers to identify and mitigate cyber risks, it is not intended to be an exhaustive list of requirements and does not constitute professional advice. Insurers are expected to implement adequate and effective cybersecurity measures which are appropriate and commensurate with the size, nature and complexity of their business. Insurers should seek professional advice if they have any questions relating to cybersecurity and any matters arising from this Guideline.

4. Cybersecurity strategy and framework

4.1 Authorized insurers should establish and maintain a cybersecurity strategy and framework tailored to mitigate relevant cyber risks that are commensurate with the nature, size and complexity of their business. The cybersecurity strategy and framework should be endorsed by the Board of the insurer.

4.2 Insurers, when establishing the cybersecurity strategy and framework, may make reference to or benchmark with the technology as well as the best available and practicable quality assurance standards, taking into account of their business nature, size, complexity and risk profile. Examples of such standards may include ISO/IEC 27001, and Framework for Improving Critical Infrastructure Cybersecurity issued by National Institute of Standards and Technology of the U.S.

4.3 The cybersecurity framework should clearly define the insurer's cybersecurity objectives, as well as the requirements for competency of relevant personnel or system users. It should include well-defined processes and technology necessary for managing cyber risks and timely communication of the strategy with all users.

4.4 Insurers should review and update regularly their cybersecurity strategy to ensure that the strategy remains relevant when there is significant change in their mode of business operation or in the external business environment (including external cyber risk landscape). For example, a review should be undertaken at least on an annual basis, upon the occurrence of cyber incidents to the insurer or major external cyber events which potentially could impact the insurer, or upon the deployment of new systems or major systems changes.

5. Governance

5.1 The board of directors of an authorized insurer (the "Board") should hold the overall responsibility for cybersecurity controls and ensure accountability within the insurer by articulating clear responsibilities and lines of reporting and escalation for cybersecurity controls. It should cultivate a strong level of awareness of and commitment to cybersecurity.

5.2 The Board should establish a defined risk appetite and tolerance limit on cyber risks for the insurer and oversee the design, implementation and effectiveness of related cybersecurity programs. It may establish a designated management team to oversee and implement cybersecurity measures and controls. The designated management team should consist of members with the appropriate skills and knowledge to understand and manage cyber risks. Where the Board establishes a designated management team, the Board and the designated management team are responsible for overseeing the design, implementation and assessment of the effectiveness the insurer's cybersecurity strategy and framework and for ensuring these are continuously kept up to date.

6. Risk identification, assessment and control

6.1 Insurers should identify cyber risks and conduct assessment on the effectiveness of the mitigating measures to protect against and manage cyber risks within the risk appetite and tolerance limit set by the Board or its designated management team. A self-assessment tool for the overall cyber risk management program should be put in place, as part of an enterprise risk management program, which should encompass:

(i) identifying business functions, activities, products and services and maintaining a current inventory or mapping of its information assets and system configurations, including interconnections and dependencies with other internal and external systems; and prioritizing their relative importance;

(ii) evaluating inherent cyber risks presented by users, process and technology and underlying data that support each identified function, activity, product and service;

(iii) conducting business impact analysis for cyber risk, i.e. a determination of risks and prioritization of risk responses through identification of threats, vulnerabilities, likelihood and impacts.

6.2 Insurers should regularly review and assess if changes to cyber risk mitigation processes are necessary when significant changes to organizational and operational structure and systems take place. For example, the review should be on an annual basis or upon major deployment of systems.

7. Continuous monitoring

7.1 Insurers should establish systematic monitoring processes for early detection of cybersecurity incidents; regularly evaluate the effectiveness of internal control procedures; and update the risk appetite and tolerance limit as appropriate.

7.2 There should be effective monitoring measures including, among others, network monitoring, testing, internal audit and external audit.

7.3 As part of the monitoring process, insurers should manage the identities and credentials for physical and remote access to information assets. They should recognize signs of a potential cyber risk, or monitor if an actual breach has taken place in their systems.

7.4 Insurers should test all elements of their cybersecurity framework to determine their overall effectiveness at least on an annual basis. Insurers can use one or a combination of the latest available methodologies and practices, for example vulnerability assessment, scenario-based testing and penetration test.

8. Response and recovery

8.1 Insurers should develop a cybersecurity incident response plan, which covers scenarios of cybersecurity incidents and corresponding contingency strategies to maintain and restore critical functions and essential activities in such scenarios. This should also include criteria for the escalation of the response and recovery activities to the Board or its designated management team.

8.2 In case of a cybersecurity incident, insurers should assess the nature, scope and impact of the incident and take all immediate practicable steps to contain the incident and mitigate its impact.

8.3 Insurers should notify internal stakeholders, and where applicable, external stakeholders and consider joint incident response actions, if necessary. In this regard, insurers should perform incident response drill at least on a yearly basis.

8.4 Upon the detection of a relevant incident, the insurer should report the incident with the related information to the IA as soon as practicable, and in any event no later than 72 hours from detection.

8.5 Once stable operations are resumed, insurers should identify and mitigate all vulnerabilities that were exploited, and remediate the identified vulnerabilities to prevent similar incidents as part of their recovery process from the relevant incident.

9. Information sharing and training

9.1 Insurers should establish a process to gather and analyse relevant cyber risk information and participate in information sharing groups, e.g. information sharing intelligence platform, for timely information sharing to allow spontaneous and appropriate precautionary measures to be taken in combating cyber-attacks and other forms of cyber risks, both locally and internationally.

9.2 Cyber risks and vulnerabilities evolve rapidly, as do best practices and technical standards to address them. Insurers should arrange adequate training for all system users on the subject of cybersecurity awareness and the latest developments in cybersecurity, taking into account the type and level of cyber risks they may face. Insurers are encouraged to promote the professional competence and capacity of their staff, especially those responsible for cybersecurity and systems.

10. Implementation

10.1 This Guideline shall take effect from 1 January 2020.

June 2019