Suruhanjaya Sekuriti
Securities Commission
Malaysia

PUBLIC RESPONSE PAPER

NO. 1 /2016

REGULATORY FRAMEWORK FOR CYBER SECURITY RESILIENCE

The Securities Commission Malaysia (SC) issues this Public Response Paper in response to feedback received pursuant to the Public Consultation Paper on the proposed regulatory framework on Cyber Security Resilience dated 21 March 2016.

This Public Response Paper is dated 31 October 2016

1. INTRODUCTION

1.1. Effective management of cyber risk is critical given the potential disruptive effect of a cyber breach on the smooth functioning of the capital market, considering the inter-linkages of roles played by market institutions and capital market participants (collectively referred to as capital market entities). Vigilance in the management of cyber risk is also important to protect investors' confidential data, which is key to preserving market confidence.

1.2. The SC published a Public Consultation Paper on 21 March 2016 to invite feedback from interested parties on the proposed regulatory framework for management of cyber risk. The Public Consultation was closed on 29 April 2016.

1.3. A total of 41 of respondents, which include financial groups, commercial and investment banks, Capital Markets Services Licence (CMSL) holders, IT security vendors, trade associations, and individuals have responded to the Public Consultation Paper. Respondents were generally supportive of the SC's principles-based and proportionate regulatory approach to cyber risk management applicable to various capital market entities with different organisational structure, nature of potential risk exposure and impact.

1.4. The SC would like to thank all respondents for their valuable and constructive feedback and suggestions, which have been duly considered in the finalisation of the regulatory framework. The finalised requirements are provided in the *Guidelines on Management of Cyber Risk* (Guidelines).

1.5. Key feedback from the industry and SC's responses are summarised in the following sections.

2. KEY FEEDBACK AND RESPONSES

2.1. Cyber risk policy and resources at the group level

2.1.1. In the Consultation Paper, the board of capital market entities is required to provide oversight, approve cyber risk policy and review the effectiveness of policy implementation. Board is also required to ensure adequate resources are allocated, including identifying a dedicated senior officer responsible or other appropriate structure, for managing cyber risk.

2.1.2. Some respondent, particularly market intermediaries operating within a financial group, sought clarifications whether adoption of cyber risk policy approved by group board and leveraging on IT and cyber security personnel centralised at the group level would meet SC's requirements, instead of sourcing for additional personnel at the subsidiary level.

2.1.3. The SC wishes to clarify that capital market entities operating under a financial group may leverage on the group's cyber risk policy, provided that such policy is sufficiently comprehensive and addresses key areas specified in the Guidelines. Where cyber risk management functions and resources are centralised at the group level, such practices would be considered as meeting the requirement of the Guidelines.

2.2. Monitoring of third party service providers' compliance to capital market entities' internal cyber risk policy

2.2.1. In the Consultation Paper, the SC proposed that a capital market entity must ensure that third party service providers who are engaged in the system development, network monitoring, IT infrastructure maintenance, etc. comply with the capital market entity's internal IT security policy.

2.2.2. Several respondents highlighted that it may be challenging to monitor third party service providers' compliance to their IT security policy due to the lack of resources. Some respondents have also suggested that the SC extends the application of the proposed framework to third party service providers to encourage compliance.

2.2.3. The SC wishes to clarify that capital market entities will remain accountable to continuously monitor potential cyber risk that may arise from the outsourcing of IT functions to a third party service provider and require such third party service provider to adhere to their internal IT security policy.

2.2.4. This is reflected in the requirements of the Guidelines which require a capital market entity to undertake comprehensive assessment of potential vulnerabilities within its operating environment, including making an assessment of potential vulnerabilities relating to the personnel, parties with whom an entity deals with, systems and technologies adopted, business processes and outsourcing arrangements.

2.3. **Adoption of international IT standards**

2.3.1. A majority of the respondents agreed to the adoption of ISO 27001 standards as a benchmark of sound practices. Nonetheless, several respondents suggested flexibility to adopt other similar international standard, such as the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), in line with the parent company practice. There were also recommendations to benchmark against specific standard such as the ISO 27032: 2012 Guidelines for Cyber Security.

2.3.2. The SC encourages alignment of capital market entities' practices to the ISO 27001 as a best practice, in view of the standard adopted in the National Cyber Security Policy. Nonetheless, the SC also takes note that international standards may be subject to change as better practices emerge and the complexity of cyber security challenges evolve over time. Therefore, the SC does not intend to prescribe a particular mandatory international standard that a capital market entity must adopt and has no objection to market entities benchmarking their practices to alternative international standards given the common objective of international IT security standard towards ensuring cyber resilience.

2.4. **Request for extension of compliance timeline**

2.4.1. A number of respondents have requested for longer transition arrangements to ensure internal readiness for full compliance.

2.4.2. The SC has taken into consideration the need to allow appropriate transition arrangements and balancing with the need to ensure that systematically important institutions in the capital market fully comply with the requirements of the Guidelines in early stages. Accordingly, the implementation timeline is revised as follows:

Capital market entities	Compliance by
Capital market entities identified by the SC	March 2017
Holders of Capital Markets Services Licence for: • Dealing in securities • Dealing in derivatives • Dealing in private retirement scheme • Advising on corporate finance; and/or • Fund management that are not identified to comply by March 2017	December 2017
All other capital market entities • Capital Market Services Licence holders for: ○ Investment advice; and/or ○ Financial planning • Bond pricing agency • Credit rating agency • Trustees • Self-regulatory organisation • Private Pension Administrator • Registered market operators.	December 2018

2.5 Implementation of cyber risk information platform sharing

2.5.1 The SC sought feedback on the proposed initiative to establish a cyber risk information sharing arrangement and the scope of information on cyber incidents to be reported to the SC to enhance market awareness of and preparedness against cyber threats.

2.5.2 Generally, respondents were agreeable to the initiative on the information sharing arrangements given benefits to the overall capital market and recommended the SC to provide further clarity on the implementation approach.

2.5.3 A number of respondents recommended the SC to develop standard reporting requirements, including among others, the nature of cyber incident, details on the source of attack and impact to the systems and information assets of the capital market entities to be reported to the SC. Respondents also highlighted the need to ensure that the confidentiality of sensitive data reported to the SC should be preserved.

2.5.4 Details on when a cyber incident should be reported to the SC and the scope of reportable information, including operational guidance and example of cyber incident reporting are provided in Appendix 1 of the Guidelines. The SC may review the adequacy of information that should be reported from time to time, as necessary.

2.5.5 In the long run, the SC intends to centralise the reporting of cyber incidents via an electronic platform to provide a secured and efficient mean for incident reporting, which is expected to be completed in 2017. In the interim, any cyber incidents are to be reported via secured email to cyberreporting@seccom.com.my.

2.5.6 The SC is committed to ensure that confidentiality of sensitive data reported to the SC are protected and intend to share the nature, trends and sources of cyber threats through periodic engagements with the capital market industry. Further details on arrangements for the industry engagement will be communicated to the industry at a later stage.