Suruhanjaya Sekuriti
Securities Commission
Malaysia

PUBLIC CONSULTATION PAPER

NO. 1/2016

PROPOSED REGULATORY FRAMEWORK ON CYBER SECURITY RESILIENCE

The Securities Commission Malaysia (SC) invites your written comments to this consultation paper. Comments are due by **29 April 2016** and should be sent to:

Institution Supervision Department

Securities Commission Malaysia

3 Persiaran Bukit Kiara, Bukit Kiara 50490 Kuala Lumpur

E-mail : cyberconsult@seccom.com.my

Fax : + 603-6201 5208

Additional copies of this document may be made without seeking permission from the SC or downloaded from its website at www.sc.com.my

Confidentiality: Your responses may be made public by the SC. If you do not wish for all or any part of your response or name to be made public, please state this clearly in the response. Any confidentiality disclaimer that may be generated by your organisation's IT system or included as a general statement in your fax cover sheet will be taken to apply only if you request that the information remain confidential.

The SC agrees to keep your personal data confidential and in full compliance with the applicable principles as laid under the *Personal Data Protection Act 2010* (PDPA).

This Public Consultation Paper is dated 21 March 2016

CONTENTS

Page

1. Overview……3

2. The SC's proposed regulatory approach for cyber security……..4

3. Governance of cyber security risk……5

Roles and responsibilities of board of directors……5

Roles and responsibilities of the management……6

4. Establishing an internal cyber security policies and procedures…….. 7

5. Management of cyber security risk……8

Prevention…… 9

Detection……..10

Recovery……..11

6. Alignment to international information security standards……..12

7. Information sharing platform……13

8. Implementation plan and transitional arrangements……..14

1. Overview

1.1 This consultation paper is intended to generate discussion and seek feedback from interested parties in relation to the SC's proposed regulatory framework for capital market participants' management of cyber security risk.

1.2 The rapid growth in innovation and technological developments in financial markets and services have delivered substantial productivity improvements in markets both in Malaysia and globally. In the capital market, the advancement of information technology development plays a significant role in contributing to improved productivity and efficiency, and is widely deployed in many parts of the capital market value chain.

1.3 While the significant benefits of information technology are well recognised, greater dependency by capital market participants on information technology and Internet connectivity has also given rise to increased cyber security risk exposure, which may in turn raise concerns regarding the protection and preservation of the confidentiality, integrity and availability of information systems.

1.4 Effective cyber security risk management is critical given the potential effect on the broader capital market system as market participants are closely interlinked and interdependent to one another.

1.5 For example, interruptions to an exchange's operation including its electronic trade matching and execution, price dissemination and clearing facilities are likely to disrupt the smooth functioning of the market and may trigger systemic implications. Interference with vital stockbroking systems such as those providing online trading accounts, direct market access (DMA) and online payments may affect investor trading activity and potentially compromise sensitive client information which could lead to the deterioration in investor confidence.

2. The SC's proposed regulatory approach for cyber security

2.1 The SC views sound management of cyber security risk as a key priority to further strengthen the resilience of the Malaysian capital markets.

2.2 Towards this objective, the SC is proposing to introduce regulatory requirements to guide the capital market participants achieve a certain state of cyber security resilience that commensurate with their cyber security risk exposure and impact. This framework also seeks to enhance the awareness and understanding of cyber security risk among capital market participants.

2.3 This consultation paper outlines the proposed requirements and consultation questions to solicit views and feedback from interested parties, which would facilitate the SC's further engagements and discussions with market participants, prior to finalising the regulatory framework. Key regulatory requirements covered in this consultation paper include –

I. roles and responsibilities of the Board and senior management in having oversight and managing cyber security risk;
II. establishment of internal cyber security policies and procedures that should be developed by the capital market participants; and
III. measures for managing of cyber security risk.

2.4 The proposed regulatory requirements will be imposed on all capital market participants that are regulated by SC be it via licensing, authorisation, approval or registration as required under securities laws. Among others, these will include approved stock exchange i.e. Bursa Malaysia, licence holders, registered persons and self-regulatory organisation (SRO) under securities laws.

3. Governance of cyber security risk

3.1 Cyber security risk events may have significant impact both from a strategic and capital market system perspective (e.g. loss of market confidence and market share).

3.2 The SC is of the view that the board of directors of capital market participants play a critical role in setting direction at the strategic level and giving adequate priority in board agenda and allocating resources for effective management of cyber security risk.

Roles and responsibilities of board of directors

3.3 Cyber security breaches may have significant impact on the smooth functioning of day-to-day capital market services and operations as well as business reputation and sustainability.

3.4 It is crucial that the board of directors possesses a good understanding of cyber security risk and its impact on the organisation, accords sufficient priority to, and provides sufficient oversight of cyber security risk as part of the organisation's overall framework for managing risk.

3.5 The SC is proposing the following scope of roles and responsibilities that should be undertaken by board in governing cyber security risk. Among others, the Board shall ensure–

(a) that it approves the capital market participant's policies and procedures relating to cyber security;

(b) the management establishes and implements board approved cyber security policy;

(c) adequate resources are allocated for managing cyber security risk. This may include identifying a dedicated senior officer responsible or other appropriate and effective organisational structure for managing cyber security risk;

(d) management continues to promote awareness on cyber security resilience throughout the institution and closely monitor the implementation of cyber security measures;

(e) the effectiveness of the implementation of the institution's cyber security policies is periodically reviewed and corrective actions are taken to improve existing policies and cyber security practices; and

(f) the board or the relevant board committee is updated from time to time and aware of new or emerging trend of cyber security threats given the evolving nature of cyber security risk, and understand the potential impact to the organisation (e.g. specific parts of the business and operations that may be affected, consequences and potential cost of data confidentiality and integrity breaches, applicable regulatory sanctions, the extent of financial losses and potential liabilities, etc.)

Roles and responsibilities of the senior management

3.6 Effective governance of cyber security risk requires the support of the senior management in developing and most importantly, implementing cyber security policy and operational procedures that is appropriate to the nature of business operations and cyber security threats.

3.7 The SC places particular accountability on the senior management to develop an appropriate framework for managing cyber security risk as well as putting in place awareness programme and risk reporting mechanism to support the board's oversight of cyber security risk

3.8 The SC is proposing the following scope of responsibilities on the senior management as part of the requirements of the guidelines. The senior management shall–

(a) establish and implement a cyber security policy that commensurate with the level of cyber security risk exposure and its impact to the organisation. The policy shall take into account the sensitivity and confidentiality of data, vulnerabilities of information systems and the operating environment, the existing and emerging cyber security threats in determining the appropriateness of its cyber security policy and measures to be implemented;

(b) ensure that staff are aware and understand cyber security risk exposures and risk management policies and procedures of the organisation;

(c) update the board from time on new and emerging cyber security threats and their potential impact to the organisation; and

(d) propose recommendation to the board on appropriate strategies and measures to respond to cyber security risk including making necessary changes to policies and procedures, as appropriate.

4. Establishing an internal cyber security policies and procedures

4.1 A capital market participant is expected to establish and implement cyber security policies and procedures which are relevant in the context of the organisation and commensurate its risk profile, sufficiently comprehensive covering critical aspects of cyber security risk management and well-defined to ensure effective implementation at individual organisation. Clear documentation of policies and procedures would also facilitate the SC's supervisory assessment of individual organisation's approach to managing cyber security risk.

4.2 The SC is proposing that the policies and procedures put in place by capital market participants should, at the minimum, address the following areas:

(a) Clear description of the level of cyber security risk that is tolerable to the organisation (e.g. maximum service downtime, recovery time objectives, occurrence and severity of cyber security breaches, minimum level of system and services availability or a combination of other relevant risk tolerance measures);

(b) Strategy and measures to prevent, detect and recover from cyber security breaches;

(c) Roles, responsibilities and accountabilities of key personnel identified to manage cyber security risk, including the chief information security officer, chief technology officer, heads of business units, internal audit risk management, business continuity management and the board or board committee, where relevant;

(d) Processes and procedures for the identification, assessment and escalation of cyber security breaches, and the internal decision-making process;

(e) Processes and procedures for the management of outsourcing, system development and maintenance arrangements with third party vendors or service providers including requirements for third party vendors or system providers to comply with the organisation's information security standard; and

(f) Communication procedures that will be activated in the event of a cyber attack which include information contents, communication channels, list of internal and external stakeholders and communication timeline.

5. Management of cyber security risk

5.1 Given the continuous evolution nature of cyber attacks, it is important that capital market participants remain vigilant in their approach to managing cyber security risk. While most capital market participants would have in place some

form of preventive measures such as deployment of anti-virus and malware programmes, building firewall and implementing access control measures, market participants should also have capabilities to continuously detect breaches and be able to recover from a cyber security event.

5.2 The SC is proposing that capital market participants should take a combination of prevention, detection and recovery measures as outlined in the following section.

Management of cyber security risk

Prevention

5.3 Capital market participants should conduct regular assessments to identify cyber security vulnerabilities that may be exploited by internal or external threats, which could undermine the security, confidentiality, availability and integrity of the information and systems maintained and / or operated by the capital market participant, vendor or outsourced to a third party.

5.4 Capital market participants should set and implement preventive measures to minimise exposures to cyber security risk. For example, this may include deployment of anti-virus software to detect and isolate malicious code, layering systems and systems components and build firewalls, reducing weak points through which attacker can gain access to an institution's network, rigorous testing at software development stage to limit the number of vulnerabilities, penetration testing of existing systems and networks and the use of authority matrix to limit privileged internal or external access to systems

5.5 Staff, including the Board and management should undergo appropriate training on a regular basis to increase overall awareness and enhance preparedness to deal with a range of cyber security risk scenarios

5.6 Capital market participants should take into consideration that implementation of preventive measures alone may not be sufficient given that the evolving nature of cyber security threats and may need to be combined with active detection and recovery strategies.

Detection

5.7 Capital market participants must monitor for any cyber security breaches within systems and networks operated or managed by the participant or an appointed third party, notwithstanding that preventive measure may already be implemented.

5.8 Detected breaches should be escalated to an incidence response team and management in accordance to the communication processes and procedures of individual market participant and determine an appropriate response. Concurrently, any detection of cyber security breaches should be reported to the SC CERT.

5.9 Capital market participants should note that that timely detection of and response to cyber security breaches within a clearly defined escalation and decision-making processes are highly critical to ensure that any adverse effect of a cyber attack is not prolonged and recovery action can be initiated quickly.

5.10 To ensure sufficient preparedness to respond to cyber security incidences, capital market participants shall–

(a) identify common cyber incidences that the organisation is most likely to be exposed to facilitate development of a incidence response plan;

(b) assess the likely impact of these incidences;

(c) plan appropriate responses and communication strategies (incidence response plan) that may be taken.

5.11 Common cyber incidences should be reviewed and updated from time to time to reflect changes to and emergence of new cyber security threats.

Recovery

5.12 Capital market participants should aim to achieve a state of cyber resilience whereby systems that they operate are able to absorb shock of a cyber attack without totally breaking down. This means systems should be able to recover from a cyber attack at a reasonably short period of time to provide critical services or some level of minimum services in a degraded state for a temporary period.

5.13 Based on the capital market participants' system profile, participants should identify what critical systems and services should be prioritised and recovered to provide certain minimum level of services during the downtime and determine how much time is required to return to full service and operations.

5.14 The business continuity plan (BCP) of a capital market participant should be sufficiently comprehensive and include a recovery plan for systems and operations in the event of a cyber attack. For the avoidance of doubt, capital market participants may build on the organisation's existing BCP to incorporate recovery plan in response to cyber attack.

5.15 The SC recognises that measures and approaches adopted by individual organisation in dealing with cyber security risk may differ across a diverse range of capital market participants.

5.16 The SC intends to take a proportionality approach in the assessment of compliance programmes instituted by individual capital market participants, having regard to different types of capital market participants, materiality of systems and information assets, vulnerabilities of systems, network and operating environment as well as the potential impact of cyber security threats.

These considerations will be weighed against the appropriateness of measures and controls implemented by capital market participants and their expected outcomes in term of cyber resilience.

Question 1:

Do you foresee any implementation issues and challenges with regard to the proposed cyber security risk management measures above? Please describe the specific issues and rationale in detail.

Question 2:

Do you have any suggestions on alternative approach to managing cyber security risk effectively?

Question 3:

What strategy and approach would your organisation take in dealing with new or unknown cyber security, notwithstanding that your organisation may have identified responses to common cyber security threats?

Question 4:

In your assessment, what are the key systems and information assets in your organisation that should be recovered on a priority basis and be able to provide certain minimum level of services in the event of cyber attack? Please provide details on the type and purpose of these systems and information assets, where relevant.

6. Alignment to international information security standards

6.1 Consistent with the National Cyber Security Policy and international practices, the SC is proposing that capital market participants should also observe sound practices under the ISO 27001 standard. The SC is of the view that capital market participants' observance to international information security standard would provide a benchmark to assess current cyber security risk management capabilities and develop internal priorities and roadmap.

6.2 For the avoidance of doubt, the SC does not require capital market participants to obtain an independent certification for their compliance to the ISO standard.

Question 5

Do you agree with the proposed adoption of the ISO 27001 standard as the international standard for purposes of assessing internal capabilities and setting cyber security initiatives and priorities? If not, please provide the specific implementation issues and justification.

7. Information sharing platform

7.1 A cyber security risk event that materialised at one capital market participant may also be relevant to and affecting another participants in the capital market system. Effective cyber security threats and intelligence sharing among capital market participants would enable market participants to -

(a) advance their awareness about current and emerging cyber threats;
(b) understand better the impact to their organisation;
(c) collaborate with other participants; and
(d) take pre-emptive measures.

7.2 The SC is proposing to establish a cyber security information sharing platform, building on the existing mechanism for the reporting of cyber security to the SC-CERT. The proposed platform is envisaged to provide a secured environment to capture key cyber attack information affecting the capital market industry and to enable users of the platform to improve their defences against such threats such as undertaking own penetration test using on new cyber security threats scenario.

Question 6

What specific information contents that should be available to users of the platform in order to enable market participants to improve defences against cyber security threats while maintain confidentiality of certain sensitive information?

Question 7

What are the key issues and challenges that should be addressed for the information sharing arrangement to be implemented?

8. Implementation plan and transitional arrangements

8.1 The SC expects to finalise the regulatory framework by second quarter of 2016, after taking into consideration industry feedback on the proposed framework. The SC may also hold industry focus group discussions before the finalisation of the framework to assess the level of industry readiness to implement the requirements.

8.2 Once finalised, the regulatory requirements must be complied with by all capital market participants based on the following phases:

Phase	Timeline	Capital market participants
Phase 1	Q1 2017	• Bursa Malaysia • Holders of CMSL for dealing in securities • Holders of CMSL for dealing in derivatives
Phase 2	Q1 2018	• All capital market participants

8.3 Prior to the effective compliance date, capital market participants are generally expected to build the necessary capacity and competency, initiate development of strategies and plans for managing cyber security risk with participation of senior management and board or the relevant board committees, and promote internal

awareness among staff about cyber security risk and its impact, approach and policies to the organisation in dealing with cyber security threats.

Question 8:

Are there any specific issues and challenges for your organisation to comply with requirements of the proposed guidelines and implementation timeline? Please describe the specific implementation issues and justification in detail.