GUIDELINES ON MANAGEMENT OF CYBER RISK

SC-GL/2-2016

1st Issued: 31 October 2016

Suruhanjaya Sekuriti
Securities Commission
Malaysia

GUIDELINES ON MANAGEMENT OF CYBER RISK

Effective Date upon 1st Issuance:	31 October 2016

CONTENTS

Page

PART A: GENERAL **1**

Introduction 1

Definitions **2**

PART B: GOVERNANCE OF CYBER RISK **4**

Roles and responsibilities of the board of directors 4

Roles and responsibilities of the management 5

PART C: MANAGEMENT OF CYBER RISK 6

Cyber risk policies and procedures 6

Cyber risk measures 7

Prevention 7

Detection 8

Recovery 9

APPENDIX 1 ..... **10**

PART A: GENERAL

Introduction

1.1 The *Guidelines on Management of Cyber Risk* are issued pursuant to section 377 of the *Capital Market and Services Act 2007* (CMSA).

1.2 These Guidelines shall apply to all capital market entities.

1.3 These Guidelines set out the following requirements:

(a) Roles and responsibilities of the board of directors and management in the oversight and management of cyber risk;
(b) Cyber risk policies and procedures that should be developed and implemented by capital market entities;
(c) Requirements for managing cyber risk; and
(d) Reporting requirements to the Securities Commission Malaysia (SC).

1.4 These Guidelines are in addition to and not in derogation of any other guidelines issued by the SC or any requirements as provided for under securities laws.

1.5 The SC may, upon application, grant an exemption from or a variation to the requirements of these Guidelines if the SC is satisfied that–

(a) such variation, if granted is not contrary to the intended purpose of the relevant requirements in these Guidelines; or

(b) there are mitigating factors which justify the said exemption or variation.

Definitions

2.1 Unless otherwise defined, all words used in these Guidelines shall have the same meaning as defined in the CMSA. In these Guidelines, unless the context otherwise requires–

agent	means any person representing or acting for the entity such as a remisier or a unit trust consultant;
board	includes board committee;
business continuity	means a state of uninterrupted business operations;
capital market entity (entity)	means capital market institutions or participants licensed, authorised, approved or registered under the securities laws;
cyber incident	means an observable occurrence indicating a possible breach in the systems, network and operating environment;
cyber resilience	means the ability to anticipate, absorb, adapt to, rapidly respond to, and recover from disruption caused by a cyber attack;
cyber risk	means the combination of the probability of an incident occurring within the realm of an entity's information assets, systems and operating environment;
cyber threat	means a circumstance or incident with the potential to intentionally or unintentionally exploit one or more vulnerabilities in an entity's information assets, systems and operating environment;
detection	means the development and implementation of the appropriate activities in order to identify the occurrence or potential occurrence of a cyber incident;

information assets	means any piece of data, device or other component of the environment that supports information-related activities;
malware	means malicious software used to disrupt the normal operation of an information system in a manner that adversely impacts its confidentiality, integrity or availability;
prevention	means safeguards, controls and measures to ensure delivery of critical infrastructure services;
recovery	means restoration of any capabilities or services that have been impaired due to a cyber incident;
recovery time objective (RTO)	means targeted duration of time which an information system and network must be recovered after a cyber breach
risk tolerance	means the amount and type of risk that an organisation is willing to take in order to meet its strategic objectives; and
third-party service providers	means an entity within the group or an external entity, to which the capital market entity has outsourced the outsourced functions and includes any subsequent service provider(s) to whom the initial service provider has further contracted the outsourced functions.

PART B: GOVERNANCE OF CYBER RISK

Roles and responsibilities of the board

3.1 The board must provide oversight and accord sufficient priority and resources to manage cyber risk, as part of the capital entity's overall risk management framework.

3.2 In discharging its oversight functions, the board must–

(a) ensure that the capital market entity's policies and procedures relating to cyber risk are presented for the board's deliberation and approval;

(b) ensure that the approved cyber risk policies and procedures are implemented by the management;

(c) monitor the effectiveness of the implementation of the entity's cyber risk policies and ensure that such policies and procedures are periodically reviewed and improved, where required. This may include setting performance metrics or indicators, as appropriate to assess the effectiveness of the implementation of cyber policies and procedures;

(d) ensure that adequate resources are allocated to manage cyber risk including identifying a responsible person (responsible person) who is accountable for the effective management of cyber risk;

(e) ensure that the management continues to promote awareness on cyber resilience at all levels within the entity;

(f) ensure that the impact of cyber risk is adequately assessed when undertaking new activities, including but not limited to any investments decision, merger and acquisition, adoption of new technology and outsourcing arrangements; and

(g) ensure that the board keeps itself updated and is aware of new or emerging trends of cyber threats, and understand the potential impact of such threats to the entity.

Roles and responsibilities of the management

3.3 Management is responsible for–

(a) establishing and implementing cyber risk policies and procedures that commensurate with the level of cyber risk exposure and its impact to the entity. These policies and procedures must take into account the following:

(i) The sensitivity and confidentiality of data which the entity maintains;

(ii) Vulnerabilities of the entity's information systems and operating environment across the entity; and

(iii) The existing and emerging cyber threats.

(b) ensuring that employees, agents (where relevant) and third party service providers are aware and understand the cyber risk policies and procedures, the possible impact of various cyber threats and their respective roles in managing such threats;

(c) recommending to the board on appropriate strategies and measures to manage cyber risk, including making necessary changes to existing policies and procedures, as appropriate; and

(d) reporting to the board of any cyber breaches and periodically update the board on emerging cyber threats and their potential impact to the entity.

PART C: MANAGEMENT OF CYBER RISK

Cyber risk policies and procedures

4.1 The entity must have in place clear and comprehensive cyber policies and procedures, which commensurate with its risk profile.

4.2 Such policies and procedures must among others include the following:

(a) Clear description of the risk tolerance in relation to cyber risk that is acceptable to the entity such as, occurrence and severity of cyber breaches, the maximum service downtime, recovery time objectives, minimum level of system and services availability, potential negative media publicity, potential regulatory and financial impact or a combination of other measures;

(b) Strategy and measures to manage cyber risk encompassing prevention, detection and recovery from a cyber breach;

(c) Roles, responsibilities and lines of accountabilities of the board, the board committee, responsible person and key personnel involved in functions relating to the management of cyber risk (such as information technology and security, business units and operations, risk management, business continuity management and internal audit);

(d) Processes and procedures for the identification, detection, assessment, prioritisation, containment, response to, and escalation of cyber breaches for decision-making;

(e) Processes and procedures for the management of outsourcing, system development and maintenance arrangements with third-party service providers, including requirements for such third-party service providers to comply with the entity's information security policy; and

(f) Communication procedures that will be activated by the entity in the event of a cyber breach, which include reporting procedures, information to be reported, communication channels, list of internal and external

stakeholders and communication timeline.

Cyber risk measures

4.3 The entity must ensure that comprehensive strategies and measures are in place to manage cyber risk including prevention, detection and recovery measures.

4.4 Notwithstanding that the operation or maintenance of information assets, systems and network are outsourced to a third-party service provider, the entity remains responsible for ensuring compliance with the requirements in paragraphs 4.5 to 4.19 of these Guidelines.

Prevention

4.5 The entity must conduct regular assessments as part of the entity's compliance programme to identify potential vulnerabilities and cyber threats in its operating environment which could undermine the security, confidentiality, availability and integrity of the information assets, systems and networks.

4.6 The assessment of the vulnerabilities of the entity's operating environment must be comprehensive, 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.

4.7 The entity must develop and implement preventive measures to minimise the entity's exposure to cyber risk.

4.8 Preventive measures referred to in Paragraph 4.7 above may include the following:

(a) Deployment of anti-virus software and malware programme to detect and isolate malicious code;

(b) Layering systems and systems components;

(c) Build firewalls to reduce weak points through which attacker can gain access to an entity's network;

(d) Rigorous testing at software development stage to limit the number of vulnerabilities;

(e) Penetration testing of existing systems and networks; and

(f) Use of authority matrix to limit privileged internal or external access rights to systems and data.

4.9 The entity must ensure that the board, management, employees and agents undergo appropriate training on a regular basis to enhance their awareness and preparedness to deal with a wide range of cyber risks, incidents and scenarios.

4.10 The entity must evaluate improvement in the level of awareness and preparedness to deal with cyber risk to ensure the effectiveness of training programmes implemented.

Detection

4.11 In addition to implementing preventive measures, the entity must continuously monitor for any cyber incidents and breaches within its systems and network.

4.12 The entity must ensure timely detection of and response to cyber breaches within a clearly defined escalation and decision-making processes to ensure that any adverse effect of a cyber incident is properly managed and initiate recovery action quickly.

4.13 To ensure sufficient preparedness in responding to cyber incidents detected, the entity must–

(a) identify scenarios of cyber risk that the entity is most likely to be exposed to;
(b) consider incidents in the capital market and the broader financial services industry;
(c) assess the likely impact of these incidents to the entity; and
(d) identify appropriate response plan and communication strategies that should be undertaken.

4.14 The entity must regularly test, review and update the identified cyber risk scenarios and response plan. This is to ensure that the scenarios and response plan remain relevant and effective, taking into account changes in the operating environment, systems or the emergence of new cyber threats.

4.15 The entity must ensure that cyber breaches detected are escalated to an incidence response team, management and the board, in accordance with the entity's business continuity plan and crisis management plan, and that an appropriate response is implemented promptly.

4.16 The entity must report to the SC on any detection of a cyber incident which may or have had an impact on the information assets or systems of the entity, on the day of the occurrence of the incident. A report submitted to the SC under this paragraph must be made in accordance with the reporting template as provided in **Appendix 1.**

Recovery

4.17 The entity must ensure that all critical systems are able to recover from a cyber breach within the entity's defined recovery time objective in order to provide important services or some level of minimum services for a temporary period of time.

4.18 The entity must identify the critical systems and services within its operating environment that should be recovered on a priority basis in order to provide certain minimum level of services during the downtime and determine how much time the entity will require to return to full service and operations.

4.19 The entity must ensure its business continuity plan is comprehensive and includes a recovery plan for its systems, operations and services arising from a cyber breach.

APPENDIX 1

CYBER INCIDENT REPORTING TEMPLATE

Instructions

1. All entities are required to report cyber incident or breach to the SC on the day of the occurrence of the cyber incident or breach.

2. Entities are required to complete and submit the form below via email to the SC at cyberreporting@seccom.com.my.

3. The SC may require the affected entities to submit a detailed report on the cyber incident or breach, following the cyber incident or breach reported.

Table 1

Example of incident reporting

1. Contact information	
Contact details of the responsible person	
o Full name	
o Position	
o Office phone no.	
o Mobile no.	
o Email address	
Alternate contact person	
o Full name	
o Position	
o Office phone no.	
o Mobile no.	
o Email address	
Entity details	
o Entity name	
o Entity address	
o Type of entity (for example, financial institutions, participating organisation, exchange)	
o Contact no.	
o Email address	
2. Cyber incident or breach details	
o Date and time of incident or breach	1.45 am / 16 August 2016

○ Details of cyber incident or breach - Method of the cyber attack - Duration of the cyber attack	(i) Distributed Denial of Service (DDoS). (ii) Approximately 3 hours.

3. Impact to systems, assets or information	
o Affected hardware	(i) 11 desktop computers at Processing Department and 3 computer servers. (ii) Back office processing of trading transactions terminated
o Affected software	(i) PO-Back End Process System
o Affected operating system	(i) Windows 10 (ii) RH Linux ver 100.100 (iii) Windows Server 10
o Impact to stakeholders	(i) Next day client's trading and payment information not updated on the entity's Back Office System. (ii) Possible theft of client's information
o Geographical location and IP address of attacker	(i) Possible IP address 31.12.257.257, Eastern Europe

4. Resolution of cyber incident or breach	
○ What are the immediate remedial actions taken to minimise and mitigate risks from the cyber attack? ○ What is the current status or resolution of this incident or breach? ☐Resolved ☒Unresolved	(i) Internet connectivity was terminated. (ii) Entity's IT security and vendor was contacted to provide assistance to manage the situation and recommend remedial actions to be taken. (iii) Investigation on cyber breach is ongoing. More details expected within 24 hours.

Note:

The SC will maintain the confidentiality of data received.