GUIDANCE ON MANAGEMENT OF CYBER RISKS

A. INTRODUCTION

1. Overview

The digital world will continue to evolve rapidly and expand opportunities for innovation. On the flip side, the digital world also provides opportunities for exploitation by unscrupulous individuals or groups. The reliance on, and greater demand for the use of technology and the internet, together with the increasing complexity in the digital society with the use of automation and robotics in many organisations, have significantly increased concerns on cyber risks and exposures. This underlines the need for listed issuers to manage cyber risk.

The number, sophistication and complexity of cyber-attacks have magnified distinctly in recent years and are expected to further accelerate in the future. It is pertinent that listed issuers be vigilant, take steps to proactively address cyber risks within their own organisations. Listed issuers should therefore evaluate their cyber risks and focus on building cyber resilience to withstand and recover from any malicious cyber threats, attacks and incidents.

Cyber resilience is a core element of business resilience, which is the ability to respond and adapt quickly to disruptions or significant unplanned changes that could threaten listed issuers' operations, employees, assets or reputation. While the risk of potential cyber attack (and the resulting financial and operational impact) varies from one listed issuer to another, the general trend towards digital transformation and increasing reliance on technology means that for most listed issuers, cyber resilience is becoming the cornerstone of business resilience.

The risk of business disruption is always present. However, an effective framework of cyber risks management should be able to minimise business disruption and help listed issuers recover from adversity and return to a normal state quickly.

The Guidance on Management of Cyber Risks ("the Guidance") aims to build a culture of cyber resilience and competency among listed issuers by creating

awareness and providing guidance on cyber risks issues and measures that can be taken by listed issuers.

2. Objectives

The objectives of the Guidance are:

a) to guide listed issuers on the adoption of best practices and measures to manage cyber risk and enhance cyber resilience; and

b) to enhance awareness and understanding on the importance of cyber resilience among listed issuers.

3. Glossary

In the Guidance, the following terms have the following meanings unless the context requires otherwise:-

Term	Meaning
Bursa	Bursa Malaysia Securities Berhad
Business Continuity Plan	A comprehensive written plan of action that sets out the procedures and system necessary to continue or restore the operations of a listed issuer during any event or disruption
Cyber attack[1]	Attempts to compromise the confidentiality, integrity and availability of computer data or systems.
Cyber incident[2]	An observable occurrence indicating a possible breach in the systems, network and operating environment.

[1] As defined in IOSCO's Cyber Security in Securities Market – An International Perspective issued in April 2016.
[2] As defined in Securities Commission's Guidelines on Management of Cyber Risk issued on 31 October 2016.

Term	Meaning
Cyber resilience[3]	The ability to anticipate, absorb, adapt to, rapidly respond to, and recover from disruption caused by a cyber attack
Cyber risk[4]	The combination of the probability of an incident occurring within the realm of a listed issuer's information assets, systems and operating environment.
Cyber threat[5]	A circumstance or incident with the potential to intentionally or unintentionally exploit one or more vulnerabilities in listed issuer's information assets, systems and operating environment resulting in a loss of confidentiality, integrity or availability.
Firewall	A network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules
Incident Response Plan	A written plan that sets out incident management protocols and defines processes to manage a cyber incident once it is identified. It includes escalation procedures, remediation processes, recovery measures and if applicable, coordination with the investigatory/regulatory organizations
Information assets[6]	Any piece of data, device or other component of the environment that supports information-related activities
Malware[7]	Malicious software used to disrupt the normal operation of an information system in a manner that adversely impacts its confidentiality, integrity or availability

[3] As defined in Securities Commission's Guidelines on Management of Cyber Risk issued on 31 October 2016.
[4] As defined in Securities Commission's Guidelines on Management of Cyber Risk issued on 31 October 2016.
[5] As defined in Securities Commission's Guidelines on Management of Cyber Risk issued on 31 October 2016.
[6] As defined in Securities Commission's Guidelines on Management of Cyber Risk issued on 31 October 2016.
[7] As defined in Securities Commission's Guidelines on Management of Cyber Risk issued on 31 October 2016.

Term	Meaning
Penetration testing	A test carried out on the network and system to identify any vulnerabilities in order to ensure that the security controls employed are operating as required
Recovery Time Objective[8]	Targeted duration of time which an information system and network must be recovered after a cyber breach.
Risk tolerance[9]	The amount and type of risk that an organisation is willing to take in order to meet its strategic objectives.
Senior Management	Persons primarily responsible for the business operations of the listed issuer's core business and principal subsidiaries e.g. Chief Executive Officer, Chief Operating Officer, Chief Financial Officer.
Social Engineering	A non-technical strategy that relies heavily on human interaction which cyber attackers use to manipulate victims into performing certain actions or providing confidential information

B. MANAGING CYBER RISKS

Sound management of cyber security risk is an integral aspect in further strengthening the resilience of the Malaysian capital market. Effective cyber security risk management is a critical component that not only protects a listed issuer's reputation but also upholds the trust, confidence as well as integrity of the capital market.

The Guidance sets out the following preparations and measures that listed issuers should consider and employ to enhance their cyber resilience capabilities.

[8] As defined in Securities Commission's Guidelines on Management of Cyber Risk issued on 31 October 2016.
[9] As defined in Securities Commission's Guidelines on Management of Cyber Risk issued on 31 October 2016.

1. Governance of Cyber Risk

a) Roles and Responsibilities of the Listed Issuer's Board of Directors in the Oversight of Cyber Risk

The Board is the apex governing body of a listed issuer that is responsible for leading the listed issuer and ensuring that the interests of shareholders and stakeholders alike are protected whilst enabling the listed issuer to achieve long-term sustainability. At all times, the Board must be aware and be alert to business disruptions and emerging risks, such as digitisation and cybersecurity, and address any potential risks posed by a cyber-attack to prevent or mitigate its impacts e.g. security risk (data loss, identity theft, identity fraud, cyber threat, unauthorised physical access to premises), financial risk, operational risk, reputational risk, etc.

The Board should exercise effective oversight and institute proactive and comprehensive risk management strategies to manage cyber risk as part of the listed issuer's overall risk management framework[10]. Cyber risk must be evaluated and mitigated by putting in place effective controls. The framework should clearly define the roles and responsibilities including accountability for decision making within the organisation for managing cyber risk, including in emergencies and in a crisis.

Additionally, the Board should identify a responsible person from among the Senior Management who will be accountable for the overall effectiveness of cyber risk management. The responsible person should possess the requisite expertise and knowledge and should also have sufficient authority, independence, resources and access to the board.

[10] In line with the key principles of good corporate governance and with reference to guidance provided for Practice 10.1 of the Malaysian Code on Corporate Governance (2021), the board should evaluate key risk areas such as cyber security as well as putting in place controls to mitigate or manage those risks.

The Board is required to keep themselves updated and be aware of new or emerging trends of cyber threats, and continuously promote awareness to all levels within the listed issuer. The Board should drive the development of a robust and positive cyber risk management culture at all levels of the organisation.

Establishing a top-down strategy to manage cyber and privacy risks across the organisation is essential. As such, the Board should ensure that the Senior Management is fully engaged in making the organisation's systems as resilient as economically feasible.

b) Roles and Responsibilities of the Senior Management in the Oversight of Cyber Risk

Senior Management driving the business should take ownership of building cyber resilience. Senior Management should update the Board on cyber breaches (if any) and recommend appropriate strategies as necessary. Periodic updates to the Board on the emerging threats and their potential impact to the listed issuer are required to assist in the formulation of relevant strategies to build cyber resilience.

The role and duties of the responsible person identified by the Board should include:

i. overseeing the day-to-day management of the listed issuer's cyber risks and data management; and

ii. implementing the cyber security strategy and risk management as determined by the Board.

2. Management of Cyber Risk

a) Establishment of Cyber Risk Policies and Procedures

A listed issuer should establish clear and comprehensive cyber risk policies and procedures which commensurate with its risk profile. The established

policies and procedures should have a clear description of the risk tolerance in relation to cyber risk that is acceptable to the listed issuer. It should clearly outline the roles, responsibilities and line of accountabilities of the Board, the Board Committees, the responsible persons and the key personnel involved in the management of cyber risks in various functions within the listed issuer (e.g. information technology, risk management, business continuity, internal audit, etc). The policies should include the processes and procedures for the identification, detection, assessment, prioritisation, containment, response and escalation of cyber attacks for decision making.

b) Cyber Risk Measures

A listed issuer should ensure that comprehensive strategies and measures are in place to manage cyber risk including prevention, detection and recovery measures.

i) Prevention

The listed issuer should carry out periodic assessment to identify potential vulnerabilities and cyber threats as part of their risk management program. Relevant preventive measures e.g. anti-virus software, malware programme, firewall, rigorous testing at the point of software development, system and network penetration testing and adoption of system and data user access matrix should be implemented in order to minimise the identified cyber risk. Ongoing / regular cyber security awareness training should also be conducted as part of the efforts to enhance the level of awareness of the Board and employees of all levels.

ii) Detection

The listed issuer should undertake continuous monitoring of anomalous activity within its system and network to detect any potential cyber incidents and breaches. Detection processes and

procedures should be maintained and tested periodically to ensure awareness of anomalous events.

All cyber breaches detected should be escalated to the incident response team, Senior Management and the Board. At least one (1) member of the incident response team must be the responsible person who has been identified by the Board.

- Incident Response Plan

  When an incident does occur, a listed issuer should be prepared to document its actions. As such, a listed issuer should develop a detailed and actionable incident response plan, with clear roles and responsibilities, communication procedures and possible remediation measures.

iii) Recovery

Upon detection of a cyber attack or an attempted cyber attack listed issuer should perform a thorough investigation to determine its nature and extent as well as the damage inflicted. While the investigation is ongoing, a listed issuer should also take immediate actions to contain the situation to prevent further damage and commence recovery efforts to restore operations based on their response planning.

Clear escalation and decision-making processes are expected to be defined as part of the establishment of a comprehensive business continuity plan and crisis management plan to ensure timely recovery of its operations arising from cyber threat. Recovery time objective of each critical system should be defined according to its prioritisation and criticality.

3. Testing and Validation

A listed issuer should establish a comprehensive testing programme to validate the effectiveness of its cyber resilience framework on a periodic basis.

The listed issuer should test its response, resumption and recovery plans and processes, and include third party service providers in such exercises. The tests should address a broad scope of scenarios which, amongst others, include simulation of cyber incidents, as well as cyber breaches affecting different areas of the listed issuer's ecosystem. Where applicable, these tests should include both internal and external stakeholders of the listed issuer such as its business line management (including business continuity and incident response teams) and the relevant entities within its ecosystem. The results of the tests should be escalated to the Board and used by the listed issuer to support the ongoing improvement of its cyber resilience.

4. Learning and Evolving

A listed issuer should distil key lessons from global or local major cyber incidents, especially regarding the techniques used and vulnerabilities exploited by cyber attackers. The lessons learnt would assist the listed issuer in establishing the necessary measures to enhance and prioritise its resilience capabilities. The listed issuer should also be vigilant in monitoring global technological developments and keep abreast with the latest developments in cyber risk management in order to improve its threat detection capabilities and reduce potential employees-related security incidents.

It is crucial for a listed issuer to recognise that cyber resilience is not just confined to the information technology ("**IT**") environment. The listed issuer's IT Department should proactively engage with the Senior Management and Board in order to ensure that cyber resilience remains top priority in their agenda.

In amplification to the above, a listed issuer should ensure that its cyber risk management framework is steered towards addressing proactive protection against potential cyber incidents as opposed to providing reactive measures. Hence, the listed issuer should work towards achieving predictive capabilities and

gathering data from multiple sources to ensure that its cyber risk management framework is effective.

5. Cyber Security Awareness and Training

A listed issuer should ensure adequate focus and attention is given to enterprise-wide programs in the area of awareness and education involving Board and employees as well as third party service providers. A program of continuous development of knowledge and advanced awareness training for employees is key to an effective defence against malicious cyber activities such as attempted phishing attacks and other forms of social engineering.

In order to measure the effectiveness of cyber awareness programs, a listed issuer should carry out "random staff testing". Based on the results of the testing, the listed issuer should put in place corrective measures such as requiring staff who were unable to effectively apply what was learned during the awareness programs to undertake further training and guidance.

C. CONCLUSION

It is crucial for listed issuers to identify gaps between business ambitions and current cyber resilience maturity. All listed issuers should accord sufficient priority and resources to manage cyber risk and progressively instil a holistic "security culture" covering not just technology, but also people and processes, in order to build a cyber resilience culture in the industry and to ensure that the capital market continues to operate in a fair and orderly manner.

Listed issuers should keep abreast of latest developments in cyber security including referring to guidelines and official publications issued by Bursa and other relevant authorities.

[End]