Corporate Commercial | Technology, Media & Telecommunications

SGX RegCo Publishes Cyber Incident Response Guide for SGX-Listed Companies

Executive Summary

In October 2022, the Singapore Exchange Regulation ("**SGX RegCo**") published the Cyber Incident Response Guide ("**Guide**") to provide guidance on the best practices which are pertinent to helping issuers listed on the Singapore Exchange Securities Trading Limited ("**SGX-ST**") as well as the SGX members (collectively "**Companies**") strengthen their cyber risk management strategies and practices. The Guide aims to set out considerations and good practices for Companies to refer to in preparing and operationalising their own cyber incident response plans, and adapting these considerations and good practices as necessary to meet their own requirements.

Although the Guide does not aim to prescribe a set of standards that all Companies should adopt, it is an indication of the impact a cyber incident can have on Companies and provides a perspective on the emphasis of SGX RegCo on Companies' preparedness and response to cyber risks and incidents. Companies should promptly assess whether their existing internal policies and plans deal with cyber risks and cyber incidents, and if so, whether such policies and plans meet the SGX RegCo's expectations set out in the Guide.

Key Features of the Guide

The Guide outlines suggestions for the Companies in addressing the following key issues so that they can establish a robust cyber incident response plan.

(1) **Cyber crisis management structure**: Establishing the following teams that can be activated in the event of a cyber incident:

a. Crisis Management Team ("**CMT**") that comprises senior management (including C-suite executives and Heads of Departments of all relevant functions) and is responsible for key decision-making during a cyber incident; and/or
b. Cyber Incident Response Team ("**Cyber IRT**") that comprises key representatives from all relevant functions and is responsible for, among other things, developing, maintaining and executing a company's cyber incident response plans and any key decisions made by the CMT.

The Guide sets out a sample of the composition of a Cyber IRT and its members' roles and responsibilities.

(2) **CMT / Cyber IRT activation**: Adopting a structured approach in classifying cyber incidents to determine when CMT and the board of directors of the Companies should be activated and setting out the process for the activation of the CMT and the Cyber IRT.

(3) **CMT milestones and timelines**: Determining common milestones for updates to the CMT for each cyber scenario, and the Cyber IRT members responsible for providing these updates.

(4) **Cyber incident response lifecycle**: Establishing cyber incident response plan that charts the key considerations at key stages of the cyber incident response lifecycle which would guide a Company's actions in various cyber scenarios.

a. *Preparation* – Pre-emptive actions to prepare the Company to handle cyber incidents or prevent them. This may involve the development (including developing and maintaining a cyber playbook), and testing and validation of their plans for incident handling preparation or incident prevention.
b. *Detection and analysis* – Detect and validate a cyber security incident as well as assess and analyse the impact of a cyber attack.
c. *Remediation: Containment, eradication and recovery* – Containment and remediation of affected user accounts, networks, systems, applications or endpoints as well as containment of data breaches (if any).
d. *Post-incident* - Lessons learnt from recent cyber incidents and sharing of findings with the relevant stakeholders as soon as practicable.

Appendix B of the Guide provides sample detection, analysis and remediation activities for five common types of cyber scenarios, namely, distributed denial-of-service (DDoS) attack, phishing attack, malware/ransomware attack, data theft and leakage and website defacement. These considerations are drafted based on learnings and best practices in the industry and international standards. As a matter of good practice, it would be useful for the Company to develop specific cyber incident response playbooks for these five common types of cyber scenarios.

(5) **Good practices on crisis communications**: Developing and maintaining a robust crisis communications plan for cyber incidents and ensuring that it is aligned with their cyber incident response plans. The Guide addresses the good practices for the following areas of cyber crisis communications:

a. Roles and responsibilities of the crisis communications team ("**CCT**").
b. List of stakeholders to notify or communicate with during a cyber incident and the communication channels with these stakeholders.

c. Timeline for the activation of the CCT and the follow-up actions required (e.g. confirming communication channels to be used by the Cyber IRT, assessing the ability of the Customer Service team to handle any spikes in customer calls or walk-ins due to a cyber incident, etc.).
d. Timing or trigger for a Company to issue communications regarding a cyber incident, communication channels and the content of communications.

Disclosure of Material Information

Companies which are listed on SGX-ST are reminded of their obligations to disclose the occurrence of cyber incidents if they are considered as "material Information" under Chapter 7 of the SGX-ST Mainboard Rules and Catalist Rules (collectively, "**Listing Rules**"). Under the Listing Rules, a Company listed on SGX-ST must immediately announce via SGXNET any information known to it concerning it or any of its subsidiaries or associated companies which (1) is necessary to avoid the establishment of a false market in the Company's securities, or (2) would be likely to materially affect the price or value of its securities. When a cyber incident occurs, the Company has to assess the materiality of the incident, including the financial impact arising from the incident.

In this regard, Appendix D of the Guide sets out sample lines of messaging a Company may consider including in its communication templates in response to a cyber incident. These include best practices on the appropriate time for the Company to disclose the occurrence of a cyber incident publicly via SGXNET and/or to the media.

A Company that is subject to the requirements in the Personal Data Protection Act 2021 of Singapore ("**PDPA**") must also be mindful of its obligations to provide notification of any data breach under the PDPA to the Personal Data Protection Commission Singapore and/or affected individuals, in addition to its obligation to publicly announce and/or issue a holding statement in relation to any cyber incidents that affect the Company materially under the Listing Rules.

How Can We Help?

The specialist joint cybersecurity legal and cybersecurity team at Rajah & Tann Singapore and Rajah & Tann Cybersecurity is well placed to guide Companies in assessing and implementing their internal structures for consistency with the Guide, and assist Companies with putting in place robust plans and practices for cybersecurity preparedness and cyber incident response, including crisis communication plans that comply with the Listing Rules and the PDPA.

The joint team has in place a 24x7 standby incident response service that organisations have found of significant value in assisting them with responding to cyber incidents on a timely basis.

If you have any queries, please feel free to contact our team below.

Contacts

Rajah & Tann Singapore LLP

Corporate Commercial

Abdul Jabbar Bin Karam Din
Head, Corporate and Transactional Group

T +65 6232 0465

abdul.jabbar@rajahtann.com

Technology, Media & Telecommunications

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0786

steve.tan@rajahtann.com

Benjamin Cheong
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0738

benjamin.cheong@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications

T +65 6232 0752

lionel.tan@rajahtann.com

Tanya Tang
Partner (Chief Economic and Policy Advisor), Technology, Media & Telecommunications

T +65 6232 0298

tanya.tang@rajahtann.com

Rajah & Tann Cybersecurity

Wong Onn Chee
Chief Executive Officer, Rajah & Tann Cybersecurity

T +65 6932 2606

onnchee@rtcybersec.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

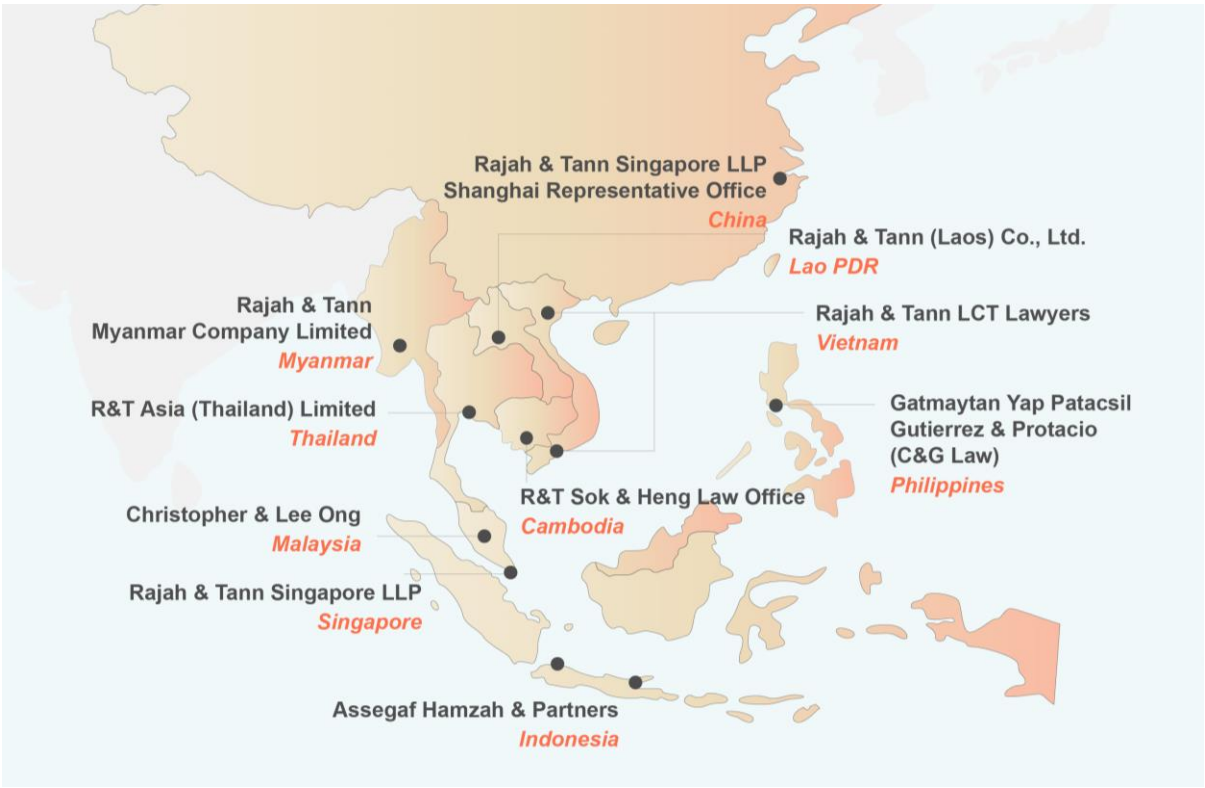
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.