Regional

China's Newly Released Draft Measures on Reporting Cybersecurity Incidents

Introduction

On 8 December 2023, the People's Republic of China ("**PRC**") issued the Draft Administrative Measures on Reporting Cybersecurity Incidents (网络安全事件报告管理办法(征求意见稿))[1] ("**Draft Measures**") for public consultation. The consultation is open for feedback on the Draft Measures until 7 January 2024.

The obligation to report cybersecurity incidents is an existing obligation for network operators under Article 25 of the PRC Cybersecurity Law (中华人民共和国网络安全法), which states that "[w]hen any incident endangering cybersecurity occurs, the relevant operator shall … report it to the competent department in accordance with relevant provisions." The Draft Measures represent a further step by the Cyberspace Administration of China ("**CAC**") to detail the reporting procedure and the potential liability for failure to meet the reporting obligation.

The Draft Measures provide additional clarity and insight into the operation of the reporting obligation. In this Update, we delve into some of the key highlights of the Draft Measures, including the scope of reportable cybersecurity incidents, the timelines for reporting, what should be included in the report, and the penalties for breach of the requirements.

Key Provisions in the Draft Measures

Definition of cybersecurity incidents

According to Article 12 of the Draft Measures, "cybersecurity incidents" are defined as those causing damage to data in a network or information system and having a detrimental impact at the societal level, regardless of whether they arise from man-made causes, software or hardware defects, or natural disasters. The severity of such cybersecurity incidents would determine the specific requirements of the reporting obligation, which will be detailed further in this article.

[1] Full text of the Draft Measures may be found here.

Regional

Classification of cybersecurity incidents

The Draft Measures categorises cybersecurity incidents into four levels based on their severity: (1) general; (2) major (较大); (3) severe (重大); and (4) extremely severe (特别重大). The specific standards for each level are set out in the Appendix I of the Draft Measures. Some examples of cybersecurity incidents that fall within each level are highlighted below:

(1) **Extremely severe**

- Overall interruption for Critical Information Infrastructure lasting over six hours or major function disruption for over 24 hours.
- Incidents impacting the work and life of over 30% of the population in a single provincial-level administrative region.
- Incidents impacting water, electricity, gas, oil, heating, or transportation supply for over 10 million people.
- Leakage of personal information of over 100 million individuals.

(2) **Severe**

- Overall interruption for Critical Information Infrastructure lasting over two hours or major function disruption for over six hours.
- Incidents impacting the work and life of over 30% of the population in a single prefectural-level administrative region.
- Incidents impacting water, electricity, gas, oil, heating, or transportation supply for over one million people.
- Leakage of personal information of over 10 million individuals.

(3) **Major**

- Overall interruption for Critical Information Infrastructure lasting over 30 minutes or major function disruption for over two hours.
- Incidents impacting the work and life of over 10% of the population in a single prefectural-level administrative region.
- Incidents impacting the water, electricity, gas, oil, heating, or transportation supply for over one hundred thousand people.
- Leakage of personal information of over one million individuals.

(4) **General**

- Incidents that pose certain threats to or have certain impacts on national security, social order, economic construction, and public interest, other than those categorised as extremely severe, severe, and major, would be deemed as general incidents.

Regional

Definition of network operators

According to Article 2 of the Draft Measures, when any cybersecurity incident occurs, the obligation lies on the network operators to report it. Network operators are defined as those who "build and operate networks or provide services through networks within the territory of the PRC". This can be contrasted against the scope of "network operation" in Article 2 of the PRC Cybersecurity Law, which refers to "the construction, operation, maintenance, and use of the network, as well as the supervision and administration of cybersecurity within the territory of the PRC". While it may appear that the definition of network operators in Article 2 of the Draft Measures is narrower, it is more prudent to take a broad interpretation of the scope of application of the reporting obligation to avoid inadvertent breach.

Timeline for reporting

Article 4 of the Draft Measures provides that, on the occurrence of any cybersecurity incident, the network operator shall promptly initiate their emergency response plan. If the cybersecurity incidents are "major", "severe" or "extremely severe", the network operator shall report the incidents within one hour (with a further 24-hour time limit for the submission of a supplemental report in certain circumstances, discussed further below).

The timeline for the reporting of "general" incidents is not specified by the Draft Measures.

Relevant regulatory agencies

For network operators other than public authorities or Critical Information Infrastructure operators, the report should be directed to the local Cyberspace Administration.

Network operators must also report to the competent industry department, if applicable. For example, the State Administration of Press, Publication, Radio, Film and Television (国家新闻出版广电总局) is the competent industry department for online publishing services, according to Article 4 of Provisions on the Administration of Online Publishing Services (网络出版服务管理规定).

In case of suspected criminal activities, network operators should also report to the police department.

Content of report

Under Article 5 of the Draft Measures, a report of a cybersecurity incident must include at least the following details:

(1) Basic information, including the name of the operator and other information regarding the facilities, systems, or platforms where the incident occurred;

(2) The time, location, type of incident, impact and harm already caused, measures taken, and their effectiveness. For ransomware attacks, the report should also include the demanded ransom amount, method, date, etc;
(3) An impact assessment of the incident, including the outlook of the situation and potential further impact and harm;
(4) Preliminary analysis of the causes of the incident;
(5) Clues needed for further investigation and analysis, including possible information about attackers, attack paths, existing defects, etc;
(6) Proposed further response measures;
(7) Protection status of the incident scene; and
(8) Other circumstances that should be reported.

Article 6 of the Draft Measures provides that if the cause, impact, or outlook of an incident cannot be determined within one hour, the network operator may first report the information specified in items 1 and 2 of Article 5, and supplement the report with other details within 24 hours.

Liability

According to Article 10 of the Draft Measures, if a network operator fails to report a cybersecurity incident as required, the CAC will impose penalties in accordance with relevant laws and administrative regulations. These relevant laws and regulations, as stipulated in Article 1, include the PRC Cybersecurity Law (网络安全法), the Data Security Law (数据安全法), the Personal Information Protection Law (个人信息保护法), and the Regulations on Security Protection of Critical Information Infrastructure (关键信息基础设施安全保护条例).

Article 10 further stipulates that in the event of significant and harmful consequences resulting from delays, omissions, concealment or the provision of false information during reporting, the network operator and relevant responsible individuals will be subject to heavier penalties in accordance with the law.

Conversely, when network operators have made their best efforts and followed the prescribed procedures, liability may be mitigated or exempted. According to Article 11, if the network operator has taken reasonable and necessary measures, voluntarily reported the incidents, and implemented the emergency response plan — making the utmost effort to minimise the impact of the incident — the liability of the network operator and relevant responsible individuals may be exempted or mitigated based on the circumstances.

Supplier

Article 8 of the Draft Measures provides that service providers of network operators, upon discovering major, severe, or extremely severe cybersecurity incidents, shall remind the network operators to report the incidents. If the network operator intentionally conceals or refuses to report the incident, the service providers can report to the local Cyberspace Administration or the CAC. However, the Draft Measures do not further specify the liability attached to the failure of service providers to remind network operators or report their omission.

Concluding Words

The Draft Measures provide welcome guidance on the procedure for reporting cybersecurity incidents, emphasising the significance of pre-planning for emergencies and the measures to be taken after an incident. Failure to report or to comply with the reporting standards may result in significant consequences for network operators, including financial and reputational impact. Further, the Draft Measures provide for mitigation and exemption of liability where best efforts have been made to comply with the reporting obligation.

It is thus advisable for network operators to develop a comprehensive emergency response plan for cybersecurity incidents and to assess their current procedures so as to avoid falling foul of the reporting requirements, as well as to stay updated on newly issued regulations and rules.

Regional

Contacts

Benjamin Cheong
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0738

benjamin.cheong@rajahtann.com

Chen Xi
Partner (Foreign Lawyer),
Rajah & Tann Singapore LLP

T +65 6232 0158

chen.xi@rajahtann.com

Linda Qiao
Head
Rajah & Tann Shanghai Representative Office

T +86 21 6120 8818

linda.qiao@rajahtann.com

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

Our Regional Contacts

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

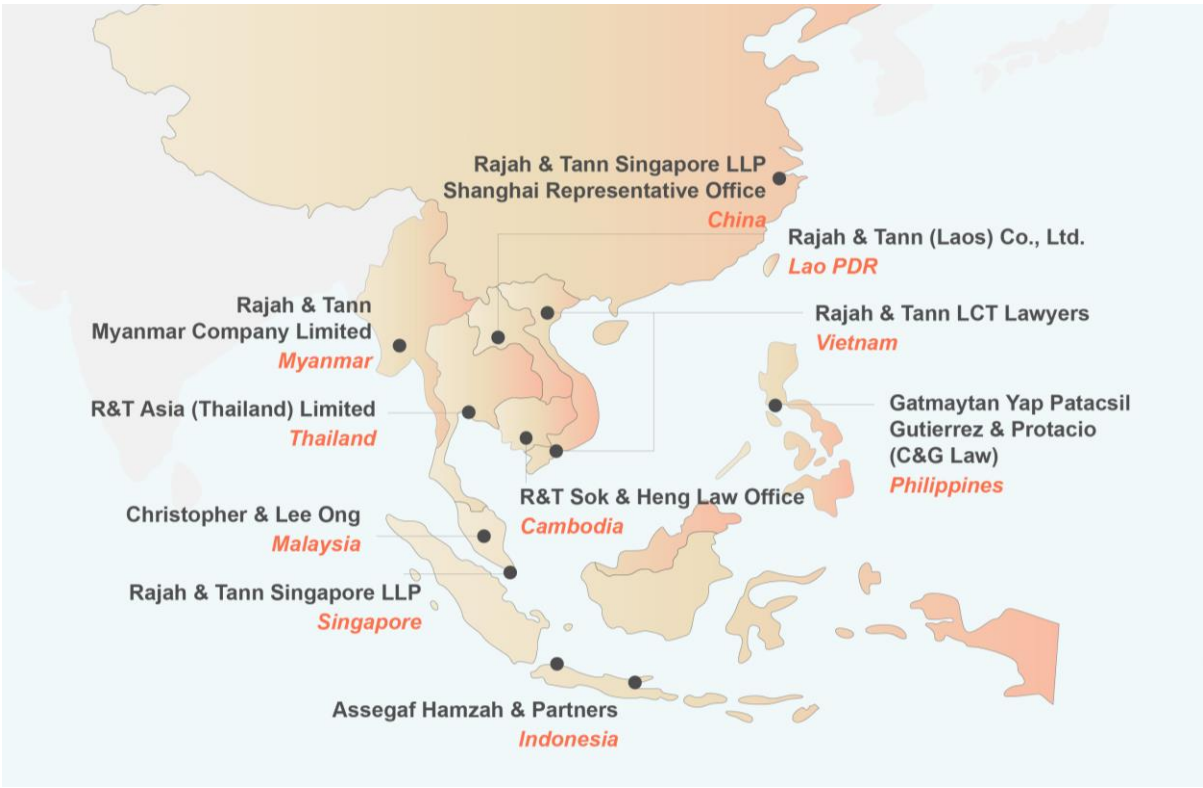
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

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.