BCLP. Client Intelligent

Insights

HONG KONG UNVEILS PROPOSALS FOR FIRST CYBERSECURITY LAW

Jul 25, 2024

SUMMARY

The Hong Kong Government recently submitted its proposed legislative framework to enhance protection of computer systems of critical infrastructure ("Proposal") to the Legislative Council ("LegCo") Panel on Security for discussion on 2 July 2024.

The Proposal notes that currently, Hong Kong does not have any statutory requirements on the protection of the computer systems of critical infrastructures ("CIs"). Given that there is an increasing risk of CIs being cyberattacked, the HK Government recognises the need to introduce new law to enhance cybersecurity of CIs.

The proposed legislation tentatively is titled the "Protection of Critical Infrastructure (Computer System) Bill".

PROPOSED LEGISLATION

WHO IS TARGETED?

The Proposal seeks to regulate CI operators ("CIOs") which are necessary for (a) the continuous delivery of essential services, or (b) maintaining important societal and economic activities in Hong Kong. In the Proposal, the HK Government states that it expects that most CIOs which are regulated would "*mostly be large organisations*".

As regards the first category (a) above (i.e. the CIOs which are necessary for the continuous delivery of essential services), the Proposal proposes to cover eight sectors: energy, information technology, banking and financial services, land transport, air transport, maritime, healthcare services and communications and broadcasting.

There is no definition as to what CIOs will fall under the second category (b) above (i.e. the CIOs which are necessary for the maintaining of important societal and economic activities in Hong

Kong), but the Proposal suggests that they could be major sports and performance venues, and research and development parks.

Not all systems within the CIOs are intended to be regulated. The Proposal only targets "critical computer systems" ("CCSs"), which are computer systems that are relevant to the provision of essential service or the core functions of computer systems which, if interrupted or damaged, will seriously impact the normal function of the CIs. The Proposal intends to cover CCSs physically located in both Hong Kong and overseas.

OBLIGATIONS?

The key obligations imposed on the CIOs under the Proposal are classified into the following three categories:

Organisational

- To keep the Commissioner's Office (further explained below) updated on the ownership and operation of the CI.
- To set up a computer system security management team with professional knowledge.

Preventive

- To update the Commissioner's Office on the CCSs and any material changes to the CCSs.
- To prepare a computer system security management plan and submit it to the Commissioner's Office.
- To conduct a computer system security risk assessment at least once every year, and submit a report to the Commissioner's Office.
- To conduct an independent computer system security audit at least once every two years, and submit a report to the Commissioner's Office.
- To adopt measures to ensure that the CCSs comply with the relevant statutory obligations even when third party services providers are employed.

Incident reporting and response

- To participate in a computer system security drill at least once every two years.
- To formulate an emergency response plan and submit it to the Commissioner's Office.
- To notify the Commissioner's Office of the occurrence of computer system security incidents in respect of CCSs within two hours (in the case of serious computer system security incidents)

or 24 hours (in the case of other incidents) after becoming aware of the incident.

COMMISSIONER'S OFFICE AND PENALTIES

Under the Proposal, a Commissioner's Office is to be set up to monitor computer system security of CCSs and ensure consistent implementation of the proposed legislation. It is proposed that the Commissioner's Office should have the powers to investigate offences under the proposed legislation, including questioning, requesting information and entering premises for investigation with a magistrate's warrant.

The proposed offences and penalty are proposed to be applicable only to the organisations, but not to their directors or staff. The maximum level of fines, depending on the seriousness of the offences, are proposed to be between HK$500,000 to HK$5 million. Additional daily fines for persistent non-compliance may be imposed.

TIMETABLE AND GOING FORWARD

The Government's plan is to introduce the proposed legislation into LegCo for consideration by the end of 2024. Upon the passage of the proposed legislation, the Government aims to set up the Commissioner's Office within one year, and to bring the proposed legislation into force within half a year's time thereafter.

In the meantime, organisations which potentially could be designated by the Government as CIOs should conduct an internal review of their existing cybersecurity systems and be ready to undergo the necessary organisational and operational changes pursuant to the proposed legislation. Given that the Proposals apply to all CCSs regardless of whether they are physically located in Hong Kong, organisations may need to bring the Proposals to the attention of their overseas offices or vendors and give some early thoughts on how to comply with the upcoming regime.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Data Center & Digital Infrastructure Team
- Digital Transformation & Emerging Technology

MEET THE TEAM

Glenn Haley

Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450

Ian Cheng

Hong Kong SAR

ian.cheng@bclplaw.com
+852 3143 8455
