

Are You Ready for the 1st Hong Kong Cybersecurity Law?

15 April 2025

OVERVIEW OF THE NEW LEGISLATION

Definitions

The new legislation, described as the first Hong Kong cybersecurity law, regulates designated “Operator of Critical Infrastructure” (the “CIO”) and its “Critical Computer Systems” (the “CCS”).

“Critical Infrastructure” (the “CI”) is defined as:

- any infrastructure that is essential to the continuous provision of an essential service in Hong Kong in eight specified sectors: energy, information technology, banking and financial services, air transport, land transport, maritime transport, healthcare services, and telecommunications and broadcasting services; or
- any other infrastructure the damage, loss of functionality or data leakage of which may hinder or otherwise substantially affect the maintenance of critical societal or economic activities in Hong Kong (e.g. major sports and performance venues, research and development parks, etc.).

An organisation that operates a specified critical infrastructure may be designated by the Commissioner as a CIO, and a computer system that is accessible by the operator in or from Hong Kong, which is essential to the core function of a critical infrastructure operated by the operator, can be designated by a designated authority or as a CCS for the infrastructure.

Certain designated authorities will be responsible for monitoring the discharge of organisational and preventive obligations by specific essential services sectors under their prevailing regulatory regimes (e.g. the Monetary Authority for the banking and financial services sector).

Obligations on CIOs

The Bill imposes the following obligations on the CIOs:

Organisational (category 1 obligations)

- maintain an office in Hong Kong;
- notify changes in the ownership and operatorship of CI; and
- set up and maintain a computer-system security management unit with professional knowledge (may be outsourced) supervised by a dedicated supervisor of the CIO.

Preventive (category 2 obligations)

- notify material changes to CCS (e.g. design, configuration, security, operation);
- submit and implement a computer-system security management plan;
- conduct a computer-system security risk assessment at least once every year; and
- conduct a computer-system security audit at least once every two years.

Incident Reporting and Response (category 3 obligations)

- participate in a computer-system security drill conducted by the Commissioner;
- submit and implement an emergency response plan; and
- notify computer-system security incidents in respect of CCS within 48 hours, save that where such incident has disrupted, is disruption or is likely to disrupt the core function of the critical infrastructure concerned, then notification must be given within 12 hours.

Regulating Authorities

A newly established Commissioner and the designated authorities will serve as the regulating authorities (the “Regulating Authorities”).

Under the new legislation, the Regulating Authorities has powers to (among others):

- ascertain whether an infrastructure is a specified critical infrastructure;

-
- designate an organisation as a CIO if the organisation operates a critical infrastructure and the infrastructure is a specified critical infrastructure;
 - designate a computer system of a CIO as a CCS if such computer system is accessible by the operator in or from Hong Kong and is essential to the core function of a critical infrastructure operated by the operator;
 - direct a CIO to do or refrain from doing an act to enforce compliance with the statutory obligations; and
 - issue codes of conduct that provide practical guidance to CIOs on compliance with the statutory obligations.

CIOs are entitled to appeal against written directions issued by the Regulating Authorities to an appeal panel that comprises, among others, information technology professionals and legal professionals. The appeal board may confirm, vary or reverse any decision to which the appeal relates, or give any direction in relation to the decision as it considers appropriate. The decision of the appeal board is final.

Commissioner's Investigation Powers

The Commissioner may direct inquiries be made to identify computer-system security threats and company-system security incidents, or direct an investigation be carried out in relation to such threats or incidents.

To facilitate the making of such an inquiry or investigation, the Commissioner can exercise various investigation powers, including the power to:

- require a CIO to produce documents, provide written responses to questions or attend an interview to answer questions;
- apply to a magistrate for the issue of a warrant to enter premises to search for and seize documents relevant to an inquiry or investigation; and
- in the context of computer-system security investigations, direct the investigated CIO or any person in control of the investigated CCS to take remedial measures or to cease carrying on any activities in relation to the threat or incident.

NONCOMPLIANCE IS AN OFFENCE

Absent reasonable excuse, failure to comply with a written request made by the Regulating Authorities in the exercise of their statutory powers is a criminal offence, with a maximum fine of HK\$5 million and a daily maximum fine of HK\$100,000 for a continuing offence, depending on the section that has been breached.

IMPLEMENTATION TIMELINE

The Bill will be implemented in phases. The Commissioner's office is expected to be established within a year after the passage of the Bill, which will come into force six months thereafter.

In anticipation of the coming into effect of the Bill within the next 18 months, stakeholders that are likely to qualify as a CIO should consider taking the steps to prepare for the changes imposed by the Bill to allow CIOs to adapt their systems, processes, and protocols to meet the new requirements effectively:

Evaluation of Impact. Be acquainted with the new requirements and their implications with a view to devising a plan to promote compliance.

Conduct Risk Assessments. Identify computer systems and infrastructures that are critical and evaluate potential vulnerabilities of these systems.

Develop Compliance Strategies. Review and upgrade existing cybersecurity policies to align with the new statutory requirements and identify and allocate resources to upgrade cybersecurity systems.

Stakeholder Engagement. Engage with relevant authorities as the Regulating Authorities provide clearer guidelines on the CIO's obligations.

IMPLICATIONS FOR COMPANIES AND ORGANISATIONS OPERATING IN HONG KONG

The Bill may have several implications for companies and organisations operating within Hong Kong.

Increased Investment Scrutiny. Stakeholders may adopt a more cautious approach towards companies operating in critical sectors, prioritising those with robust cybersecurity protocols.

Increased Costs. Compliance with the new legislation may necessitate significant investments in cybersecurity infrastructure and training, impacting the financial trajectory of organisations.

Market Opportunities. Stakeholders specialising in cybersecurity solutions may see increased demand for their services, creating potential investment avenues for private equity.

Reputation Management. Stakeholders that proactively embrace the new legislation can enhance their reputational standing, potentially attracting more investment and customer trust.

Strategic Partnerships. Collaboration between private companies and governmental bodies can foster innovation in cybersecurity practices and technologies, leading to long-term resilience in critical sectors.

In conclusion, the Bill represents a pivotal development in Hong Kong's efforts to strengthen cybersecurity in critical sectors. Its successful implementation will not only protect vital services but could also reshape the investment landscape for private equity and businesses alike.

* * *

Please do not hesitate to contact us with any questions.



Gareth Hughes
Partner, Hong Kong
+852 2160 9808
ghughes@debevoise.com



Emily Lam
Counsel, Hong Kong
+ 852 2160 9823
elam@debevoise.com



Allegra De Lorenzo
Trainee Associate, Hong Kong
+44 20 7786 5411
adelorenzo@debevoise.com