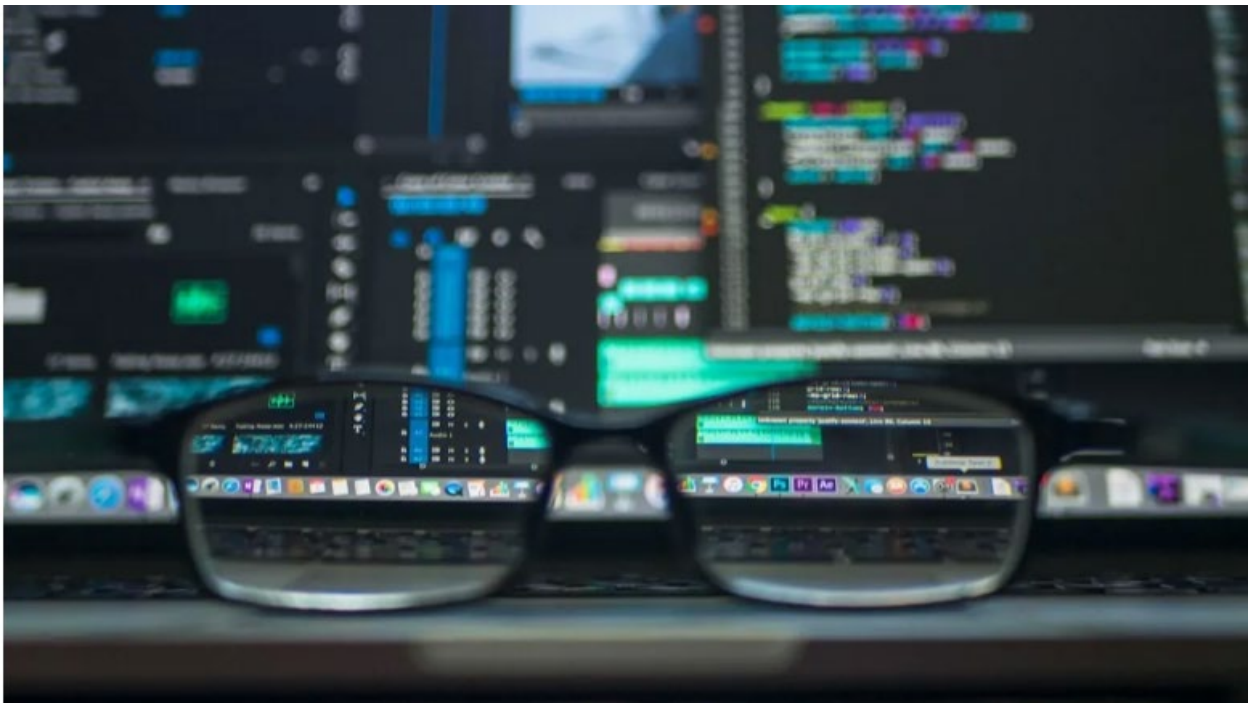
**Hong Kong's New Cybersecurity Law to Take Effect on January 1, 2026**

The Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap.653) has been enacted and will take effect on January 1, 2026.



On March 19, 2025, the Legislative Council of Hong Kong enacted the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap.653) (Ordinance), following consultation commenced in 2023. It represents Hong Kong's first comprehensive cybersecurity legislation aimed at safeguarding critical infrastructure from cyber threats and ensuring the reliability of essential services and critical societal and economic activities.

This is against the backdrop that governmental and statutory bodies like the Fire Services Department, Registration & Electoral Office, Electrical and Mechanical Services Department, the Cyberport, the Consumer Council and the Companies Registry have in recent years suffered data leaks.

The Ordinance seeks to regulate operators of crucial infrastructure that are necessary for (i) continuous delivery of essential services or (ii) maintaining important social and economic activities in Hong Kong.

The legislation will take effect on January 1, 2026, and statutorily mandates designated Critical Infrastructure Operators (CIOs) who are vital for providing essential services for day-to-day life across the eight sectors of energy, information technology, banking and financial services, land and air transport, maritime, healthcare, telecommunications and broadcasting services to adhere to specific cybersecurity protocols. It covers infrastructure facilities supporting important societal and economic activities, including major sports venues and technology parks.

The Security Bureau is setting up a new Commissioner's Office, to be appointed by the Chief Executive, and supported by designated sector-specific such as the Hong Kong Monetary Authority and Communications Authority for regulating the banking and financial services sector and the communications and broadcasting sector respectively. The Commissioner possesses wide powers to apply for a magistrate's warrant to investigate or mandate the assistance of CIO owners or third-party service providers in its investigation or response to computer system security threats or incidents in the event they are unwilling or unable to respond.

The Ordinance does not have any extraterritorial effects in its enforcement, with targets on CIOs locally. However, CIOs are required to be able to produce information to which it has access in or from Hong Kong, no matter its location.

The government also clarified that small and medium-sized enterprises and the general public will not be subject to regulation. The aim of these legal requirements is to protect the security of computer systems essential to the fundamental operations of critical infrastructure, without targeting personal data or trade secrets in any way.

Failure to comply with the obligations under the Ordinance may constitute an offence punishable with maximum fines from HK$500,000 to HK$5 million. A continuing offence will inflict a daily additional maximum fine from HK$50,000 to HK$100,000 each day. Fines under the Ordinance applies to CIOs at the organizational level and do not extend to senior management as an individual, save for any violations that may be held criminally liable for those acts such as false statements, using false instruments or other fraud-related offences.

*Organizational Requirements ("Category 1 obligations")*

CIOs must maintain a local office, notify authorities of any changes in operators, and establish a computer-system security management unit.

CIOs must establish and maintain a Hong Kong office to receive notices and other documents. Any changes to the operator (for example, a change of ownership, change in management staff members) must be promptly notified to the regulatory authorities. A dedicated unit responsible for managing the computer system security must be set up and maintained, an adequate supervisor with ample professional knowledge in the area must also be appointed to supervise the unit with his appointment notified to the Commissioner in writing.

*Preventative Cybersecurity Measures ("Category 2 obligations")*

CIOs are required to report significant changes to critical computer systems, submit and implement security management plans, conduct regular annual risk assessments and conduct biennial independent security audits.

CIOs must notify regulatory authorities of significant changes to their critical computer systems. To prevent threats and incidents, CIOs must submit and implement a detailed computer system security management plan within 3 months after the designation date. This obligation extends to any contractual arrangements engaging potential third-party service providers for computer system security management. To ensure adequate risk prevention and mitigation, CIOs are required to conduct related risk assessments at least once a year and submit a report within 3 months after each audit period to the Commission and conduct biennial independent security audit and submit a report within 3 months after each audit period to the Commissioner.

*Incident Reporting and Response ("Category 3 obligations")*

CIOs are required to participate in security exercises conducted by the Commissioner and submit and implement an incident response plan within 3 months of designation as CIO. Such incident response plan should incorporate holistic and accurate determination of cyber incident classification and severity.

They are to report any serious cybersecurity incidents, which are incidents that have or about to have a major impact on the continuity of essential services and normal operation of the CIO, or lead to a large-scale leakage of personal information and other data, to the Commissioner within 12 hours; with other incidents reported within 48 hours. A detailed written report must follow within 14 days.

This legislation marks a significant advancement in Hong Kong's cybersecurity framework, aiming to enhance resilience and ensure the uninterrupted operation of essential services amid increasing cyber threats. Organizations operating within the designated sectors are advised to proactively assess and strengthen their cybersecurity measures to comply with the new requirements and align with best practices.

As a recommendation, organizations should promptly assess whether they qualify as CIOs under the Ordinance, with the government set to designate operators in phases beginning June 2025.

Seeking legal advice at an early stage can assist in understanding the applicable criteria and obligations, as well as in reviewing and amending contracts with third-party service providers. Additionally, organizations should allocate adequate budgetary and resource provisions to develop and implement necessary security management and incident response plans, establish internal operational procedures, and conduct relevant training to ensure comprehensive compliance.

If you may be a CIO and would like to know how JML can legally support your setting up of computer systems in compliance with the legislation, scan the QR code below for access to our services.