



Protection of computer systems of critical infrastructures

Overview

Critical infrastructures (“CIs”) are the linchpin of society and economy. They are infrastructures vital to **the normal functioning of the Hong Kong society** and **people’s everyday life**, such as banking and financial institutions, communication networks, power supply facilities, railway systems and healthcare systems. Operations of these facilities will be affected, which even brings the whole society to a standstill, in case of damage or data leakage of their computer systems as a result of malicious attacks.

Other jurisdictions have enacted laws and regulations to protect the security of computer systems of CIs. Making reference to the practices in other jurisdictions, the Hong Kong Government has proposed to enact a new piece of legislation, requiring relevant operators to fulfil statutory obligations in relation to organization, prevention as well as incident reporting and response, so as to ensure the stable operation of various essential services.

This issue of **Policy Pulse** gives a brief overview of the legislative framework, and gives an account of the Administration’s responses to views received during the consultation period and relevant discussions of the Legislative Council (“LegCo”).

Legislative progress.....	[1]
Principles of legislative proposals	[2-5]
Key features of legislative proposals	[2-5]
Targets of regulation	[2]
Two categories of facilities designated as critical infrastructures.....	[2]
Computer systems designated as critical computer systems	[3]
Regulatory and enforcement authorities	[3]
Critical infrastructure operators’ three types of obligations	[4]
Investigation powers of the Commissioner and Designated Authorities	[5]
Offences and penalties.....	[5]
Relevant legislation in other jurisdictions for reference in the legislative exercise	[6]

Legislative progress




2023 :

- The Administration canvassed stakeholders’ views on the preliminary proposed legislative framework

2024 :

- July: The Administration consulted the LegCo Panel on Security and **kick-started** a one-month **consultation exercise on the proposed legislative framework**
- October: The Administration **reported the outcomes of the consultation to the LegCo Panel on Security**, and would finalize the legislative proposals having taken into account the views of Members and the industry
- December: The Administration introduced **the Protection of Critical Infrastructures (Computer Systems) Bill** into LegCo. The House Committee agreed to **form a Bills Committee** to study the Bill

Incidents of cyberattacks on certain CIs with significant impact on society in 2024

	Hong Kong	The computer system of a private hospital was attacked by hackers using ransomware, resulting in the malfunctioning of the computer system and affecting some medical services
	Sweden	A data centre was attacked by hackers, disrupting the operations of the government and businesses
	United States	A medical insurance company was attacked by ransomware; some medical services were suspended, and a large amount of personal and medical information were subject to leakage risk

Principles of legislative proposals

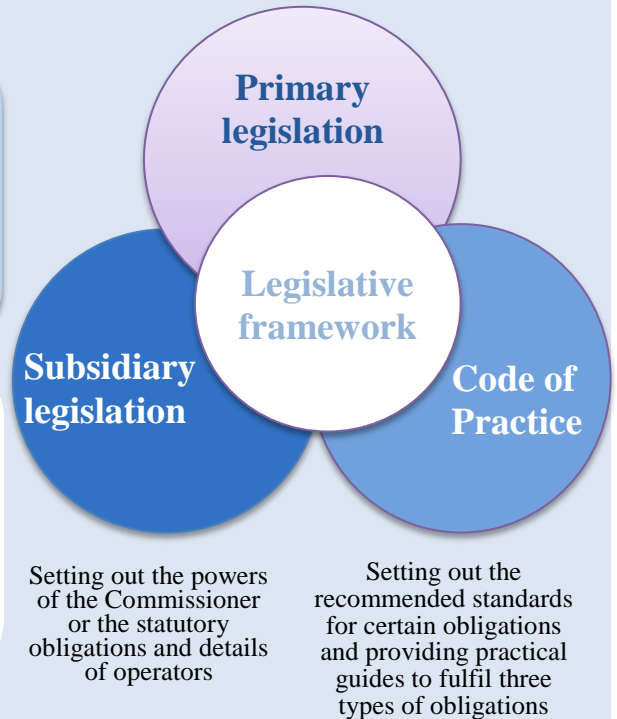
Four principles

1 Only involving designated large organizations and **not affecting individuals or small and medium enterprises**

2 Only covering operators maintaining an office in Hong Kong, **without extra-territorial effect**

3 Obtaining information for assessment and responses to incidents, without targeting at **personal information or commercial secrets**

4 Organization-based with **no personal liability** or imprisonment



Key features of legislative proposals

Targets of regulation

- **Operators of CIs** (“CIOs”) for maintaining essential services in Hong Kong or critical societal and economic activities and **their critical computer systems** (“CCSs”), which are **organization-based**
- The list of **CIOs will not be disclosed**, to prevent them from becoming targets of cyberattacks
- **Government departments** must strictly abide by the Security Regulation and the Government Information Technology Security Policy and Guidelines while the Digital Policy Office also regularly conducts compliance audits for various departments, thereby **obviating the need** for bringing government departments **under regulation**

Two categories of facilities designated as critical infrastructures

1. Infrastructures **providing essential services** in Hong Kong, covering the following **eight sectors**:
 - (1) Energy
 - (2) Information technology
 - (3) Banking and financial services
 - (4) Land transport
 - (5) Air transport
 - (6) Maritime transport
 - (7) Healthcare services
 - (8) Telecommunications and broadcasting services
2. Infrastructures for **maintaining crucial societal and economic activities**, such as major sports and performance venues, and major technology parks

Computer systems designated as critical computer systems

- Computer systems that are accessible by CIOs in or from Hong Kong
- Computer systems that are essential to the core functions of CIs

Views received during consultation: The coverage is too extensive if an interconnected computer system is designated in one go in view that the loss of its functionality may affect the provision of essential services by the operator

Post-consultation recommendation: The concept of “interconnected systems” has been deleted as the term “interconnected” may not accurately reflect the factors of consideration in designating CCSs

Regulatory and enforcement authorities

- A **Commissioner** will be appointed by the Chief Executive to head a **Commissioner’s Office** under the Security Bureau to enforce the proposed Ordinance
- The proposed Ordinance will designate the relevant industry regulators as **designated authorities**, including the **Monetary Authority and the Communications Authority** which will be responsible for regulating CIOs of the relevant sectors in fulfilling **organizational and preventive obligations**
- An independent **appeal mechanism** will be set up. Organizations that disagree with the decisions of the Commissioner’s Office in respect of CIOs or CCSs can lodge an appeal



Members’ views

- Members generally **supported** the proposed **legislative framework** put forth by the Administration.
- Members considered that the proposed Ordinance should achieve **technology neutrality**. Members were concerned that some smaller enterprises (such as data centres) might be the **third-party service providers** of CIOs and suggested the Administration to **assist these enterprises in fulfilling** the relevant **statutory obligations** under the legislation.
- As regards the non-application of the proposed Ordinance to the Government, Members suggested that **government bureaux or departments**, in particular those involved in the provision of essential services (e.g. the Water Supplies Department), must comply with **requirements of incident reporting and response** akin to that under the proposed Ordinance.
- Members suggested the Administration to, having taken into account future developments, **review** in a **timely** manner the **need to designate other statutory industry regulators**, such as the Insurance Authority responsible for regulating the insurance industry (which was a financial service sector under the proposed Ordinance), **as designated authorities** under the proposed Ordinance.

LegCo
Relevant
Paper



CIOs' three types of obligations

1 Organizational obligations

- Maintain an **office** in **Hong Kong** to facilitate compliance with obligations in relation to prevention and incident reporting and response by CIOs in Hong Kong, and notify the Commissioner or designated authorities of the address
- **Report changes** in **operatorship** of CIs to keep the Commissioner or designated authorities updated on their operation
- Set up a **computer-system security management unit** (in-house or outsourced) to ensure that a dedicated unit is in place to manage the security of computer systems and to follow up on the directions issued by the Commissioner's Office
- ✦ **Views received during consultation:** Difficulty has been expressed for organizations (in particular listed companies) to make frequent reports on change in ownership
- ✦ **Post-consultation recommendations:** The requirement for reporting changes in ownership is removed

2 Preventive obligations

- **Report material changes** in design, configuration, security or operation, etc. of CCSs
- Formulate, implement and submit to the Commissioner or designated authorities a computer-system **security management plan**
- Conduct a computer-system **security risk assessment** (at least once every 12 months) and submit a report to the Commissioner or designated authorities
- Conduct an independent computer-system **security audit** (at least once every 24 months) and submit a report to the Commissioner or designated authorities

3 Incident reporting and response obligations

- Participate in a **computer-system security drill** organized by the Commissioner's Office
- Formulate an **emergency response plan** for proper response to emergency situations and submit it to the Commissioner
- Notify the Commissioner of computer-system security incidents in respect of CCSs within the following specified time frame and submit written reports to the Commissioner within 14 days after becoming aware of their occurrence:
 - Serious incidents ^{Note} : **within 12 hours**
 - Other incidents : **within 48 hours**
- ✦ **Views received during consultation:** Difficulty has been expressed for organizations to conduct a timely investigation into the nature and cause of a serious computer-system security incident and report it to the Commissioner within two hours after becoming aware of its occurrence as required in the original proposal
- ✦ **Post-consultation recommendations:** Relaxing the time frame for reporting serious computer-system security incidents from two hours to 12 hours after becoming aware of them, and from 24 hours to 48 hours after becoming aware of other incidents

Note Meaning the computer-system security incident concerned has disrupted, is disrupting or is likely to disrupt the core function of the CI concerned

Investigation powers of the Commissioner and Designated Authorities

- The Commissioner may investigate a **threat or incident** targeting CCSs **and offences relating to the above three types of obligations**
- **Investigation powers** include requesting CIOs to answer questions and submit information, entering premises for investigation with a magistrate's warrant, etc. The above empowerment is in line with the practice of other jurisdictions. Each of these powers has specific conditions, procedures for exercising the powers, the authorizing authority, etc., to ensure that these investigation powers are kept to the minimum extent necessary

Views received during consultation:

- (1) Concern that enforcement against computer systems located outside Hong Kong may be involved
- (2) Concern that empowerment under the proposed Ordinance for the Commissioner to access equipment or install programmes in CCSs may impede the normal operation of the systems

Post-consultation recommendations:

- (1) The proposed Ordinance does not have extra-territorial effect. The information requested by the Commissioner will only be information that is accessible by operators in or from Hong Kong
- (2) Only when a CIO is unwilling or unable to respond to a serious incident on its own, etc. would the Commissioner consider applying to a magistrate for a warrant to gain access to the relevant system for responding to the incident. Relevant regulators in other jurisdictions (such as Australia and Singapore) also have similar powers

Offences and penalties

- Violations under the legislative regime constitute offences subject to the defences of “due diligence” in respect of non-compliance with the Categories 1, 2 and 3 obligations or written directions, and “reasonable excuse” for other offences
- Penalties are only **applicable to organizations**, and their heads or staff will not be penalized at individual level (unless violations touch upon existing criminal legislation, such as provision of false information)
- Maximum fines range from HK\$500,000 to HK\$5 million; for certain offences, additional daily fines for persistent non-compliance will be imposed in respect of individual offences



Members' views

- Members expressed concern about the adequate **supply of computer security professionals** and suggested that the Administration might consider establishing a list of recognized service providers for computer-system security audits to facilitate operators in engaging suitable personnel. Members were also concerned about certain **details** to be set out **in the Code of Practice**, including the compliance standards for computer-system security risk assessments and security audits to be conducted by CIOs.
- Members suggested the Administration to **clearly define** the **legal liabilities** of CIOs' **staff and third-party service providers**, and to ensure that the penalties for the proposed offences would have sufficient deterrence.

Legislation relating to protection of security of critical infrastructures' computer systems in other jurisdictions for reference in the legislative exercise



Mainland China

Cybersecurity Law of the People's Republic of China (*Chinese only*)

Regulation for Safe Protection of Critical Information Infrastructure (*Chinese only*)



The United Kingdom

Network and Information Systems Regulations 2018



Macao Special Administrative Region

Cybersecurity Law (2019) (*Chinese only*)



The United States

Cybersecurity and Infrastructure Security Agency Act of 2018

Cyber Incident Reporting for Critical Infrastructure Act of 2022



Singapore

Cybersecurity Act 2018

Cybersecurity (Amendment) Act 2024



European Union

Directive on the measures for a high common level of cybersecurity across the Union 2022



Australia

Security of Critical Infrastructure Act 2018



Canada

The relevant Bill is under consideration

Some of the issues that have been made reference to:

- In respect of the **designation of sectors of essential services** in the definition of “**critical infrastructure**”, similar practices are also found in the relevant legislation of other jurisdictions; whereas infrastructure with a similar description of sustaining critical societal and economic activities is also covered in the legislation of the United Kingdom (“UK”), Australia, the United States (“US”) and the European Union (“EU”)
- The adoption of an “**organization-based**” approach, i.e. using the organization responsible for operating a CI as the unit on which the obligations in relation to protecting the security of its computer systems are imposed, is also the practice of UK, Australia and EU
- The practice of **non-disclosure** of the **lists** of CIs and CIOs is in line with the practice of other jurisdictions such as UK and Australia
- Delegating to **industry regulators** the obligation to regulate individual CIOs is a practice that can also be found in relevant legislation of UK, Australia and US
- The **penalties** for offences of non-compliance with the obligations and requirements under the proposed Ordinance will only include fines, is a practice that can also be found in relevant legislation of UK and EU



Legislative Council
Secretariat

To know more about the related
discussions in the Legislative Council

please scan the **QR codes** on the right
or visit the relevant Legislative Council **webpages**



[Panel on Security](#)



[Bills Committee on Protection of
Critical Infrastructures
\(Computer Systems\) Bill](#)