立法會
Legislative Council

LC Paper No. CB(2)1779/2024(02)

Ref: CB2/BC/6/24

Bills Committee on
Protection of Critical Infrastructures (Computer Systems) Bill

Background brief

Purpose

This paper provides background information on the Protection of Critical Infrastructures (Computer Systems) Bill (the "Bill"), and summarizes the discussions of the Panel on Security ("the Panel") on the relevant legislative work.

Background

2. Currently, Hong Kong has no statutory requirements for the protection of computer systems of critical infrastructures ("CIs"). In the context of briefing the Panel on the relevant policy measures in October 2021, the Security Bureau advised that, in response to the increase in cyberattacks in recent years, it was proposed to clearly delineate the cybersecurity obligations for operators of critical information infrastructures through legislation. Subsequently, the Chief Executive announced in his 2022 Policy Address in October 2022 that legislation would be enacted for the enhancement of the cybersecurity of critical information infrastructures. As advised by the Administration in July 2024, having regard to the circumstances in Hong Kong, as well as drawing reference from the practices of other jurisdictions and taking into account the views of various stakeholders, the policy objective of this legislative exercise is to strengthen the security capabilities of computer systems of CIs and minimize the chance of essential services being disrupted or compromised due to cyberattacks, thereby enhancing the overall computer-system security in Hong Kong. The statistics of security incident reports received by the Hong Kong

Computer Emergency Response Team Coordination Centre ("HKCERT") from January 2018 to November 2024 are in **Appendix 1**.[1]

Protection of Critical Infrastructures (Computer Systems) Bill

3. The Bill was published in the Gazette on 6 December 2024 and received its First Reading at the Legislative Council ("LegCo") meeting of 11 December 2024. The Bill seeks to:

(a) protect the security of the computer systems of Hong Kong's CIs;

(b) regulate the operators of such infrastructures;

(c) provide for the investigation into, and response to, computer-system security threats and incidents in respect of such computer systems; and

(d) provide for related matters.

4. The key features of the legislative proposals contained in the Bill are set out in paragraphs 7 to 29 of the Legislative Council Brief (File Ref.: SBCR 1/3231/2022 Pt. 5) issued by the Security Bureau on 4 December 2024.

Members' views and concerns

Legislative framework

5. Members highlighted the rapid development of new technologies, including low-altitude flying, and pointed out that the relevant infrastructure might be involved in providing essential services for daily life in the future. In this regard, they asked how the legislative framework could **achieve technology neutrality** to cope with technological changes. The Administration advised that the proposed regulating authorities[2] might issue codes of practice ("CoPs") in respect of CI operators' obligations. In formulating and updating CoPs, the proposed regulating authorities would

[1] Managed by the Hong Kong Productivity Council, HKCERT provides local enterprises and Internet users with information on security incidents, guidance on preventive measures, incident response and support services, and promotes security awareness.

[2] See paragraph 15 below.

take into account the latest technological developments and international standards, and consult stakeholders as appropriate, so as to address various circumstances that might arise in the future.

Scope and targets of regulation

6. Members noted that the CIs to be regulated under the legislative proposals covered two major categories, namely (a) infrastructures that were essential to the continuous provision in Hong Kong of essential services in the eight specified sectors, namely energy, information technology, banking and financial services, land transport, air transport, maritime transport, healthcare services, and communications and broadcasting services; and (b) infrastructures for maintaining critical societal and economic activities. The legislative proposals would adopt an "organization-based" approach, and the proposed regulating authorities would designate the relevant organizations as CI Operators ("designated operators"). Members enquired whether electronic payment tools, instant messaging software, social media platforms, the media, radio stations, scientific research facilities of higher education institutions, and the eMPF Platform were among the proposed targets of regulation. Referring to the Administration's statement that most CIs were operated by sizable organizations, members considered it possible for some **small and medium enterprises** (e.g. small and medium-sized data centres and airlines with smaller operations in Hong Kong) to become designated operators, but these enterprises **might need support from the Administration to comply with the obligations imposed on CI operators under the legislative proposals**.

7. The Administration advised that the regulating authorities would consider multiple factors (e.g. the potential implications if a relevant infrastructure was damaged, lost functionality or suffered any data leakage) in ascertaining whether an infrastructure was a specified CI. To prevent CIs from becoming targets of attack, and drawing reference from the practices of other jurisdictions, the proposed legislation would only set out the names of the essential services sectors, instead of disclosing the list of CIs and CI operators. After the passage of the proposed legislation, the regulating authorities would designate CI operators in a phased manner having regard to the level of readiness of organizations that might be designated as CI operators in different CI sectors. In addition, the Administration would continue to strengthen the ability of small and medium enterprises to withstand cyberattacks through various measures.

8. Members enquired about the measures to be taken by the Administration to prevent members of the public from **becoming aware that an organization was a designated operator** through the Administration's prosecutions against the **proposed offences involving designated**

operators under the legislative proposals, or through **proactive disclosure by designated operators** or their **third-party service providers**. The Administration advised that when instituting a relevant prosecution, it would consider the need to apply to the court for non-disclosure of certain information during the prosecution process. The proposed CoPs issued to CI operators would set out the requirements related to the duty of confidentiality.

9. Referring to the coverage of electronic government services under the Mainland's Regulation for Safe Protection of Critical Information Infrastructure, members sought the Administration's **justifications for not proposing to bring government departments** (**in particular** those responsible for **essential services** such as **providing potable water**) **under regulation**. There were views that **the relevant departments should at least be required to comply with obligations of incident reporting and response** similar to those under the legislative proposals [3]. The Administration advised that all government departments must follow the information technology security policies and guidelines developed by the Digital Policy Office ("DPO"). These policies and guidelines, formulated based on international standards and industry best practices, were on a par with the requirements under the legislative proposals. DPO also conducted regular compliance audits for various policy bureaux and departments.

10. Members noted that all computer systems that were essential to the core function of CIs would be designated as critical computer systems ("CCSs"), regardless of whether such systems were physically located in Hong Kong. The Administration's explanation was sought on how it would **regulate computer systems located outside the territory** and **follow up** on relevant **computer-system security incidents**. The Administration advised that under the legislative proposals, in the event of a CCS experiencing a computer-system security incident, the designated operator was obliged to provide information on the computer system concerned (including systems located outside the territory that were accessible in or from Hong Kong).

Statutory obligations and penalty levels

11. The Administration proposed to impose the following three categories of statutory obligations on designated operators: organizational obligations (Category 1), prevention of threat and incident obligations (Category 2) and incident reporting and response obligations (Category 3). Regarding Category 2 obligations, the Administration proposed that designated operators must **conduct a computer-system security risk**

[3] See paragraph 11 below.

assessment at least once a year and **an independent computer-system security audit at least once every two years** and submit reports. Members sought the Administration's elaboration on the compliance standards for such assessments and audits, and whether the regulating authorities would conduct random checks of the reports received. They were concerned about **whether there were sufficient qualified information security talents** in Hong Kong to assist the designated operators in complying with the relevant statutory obligations, and suggested that the authorities **should establish a list of recognized service providers to conduct the aforesaid audits**. The Administration advised that CoPs would set out the standards for the assessments and audits, as well as the requirements for the qualifications of the audit personnel. According to its estimates, there were currently about 3 000 qualified information security personnel in Hong Kong who could provide such services. If necessary, the authorities would consider the feasibility of establishing a list of recognized service providers in the future.

12. In respect of the incident reporting and response obligations , members were concerned about **whether**, in the event of a **computer-system security incident involving leakage of personal data**, the designated operator would only be required to make a report under the mechanism of the proposed legislation, or whether it would still **be required to notify the Office of the Privacy Commissioner for Personal Data ("PCPD")** in accordance with current practice. The Administration advised that the proposed regulatory regime was not mutually exclusive with other existing legislation or practices. Designated operators should take corresponding follow-up actions in a timely manner after an incident had occurred as required or recommended by individual regulators. For information leakage incidents, the designated operators might notify PCPD according to its recommendation.

13. Members noted that the Administration intended to draw on the practices in other jurisdictions and impose maximum fines ranging from $500,000 to $5 million only at the organizational level on designated operators for the offences of non-compliance with the proposed legislation without exercising due diligence or without reasonable excuse (depending on the offence involved), with a further daily fine in the case of a continuing offence. They were concerned about whether the proposed penalties would **have a sufficient deterrent effect** on designated operators or their staff. They also sought clarification from the Administration on the **respective statutory obligations** of the designated operators and third-party service providers where the former **engaged a third-party service provider** to design or manage a CCS. The Administration advised that the purpose of introducing the relevant offences and penalties was to ensure the effective implementation and enforcement of the legislation. The legislative intent

was not to punish operators. Having regard to the actual circumstances in Hong Kong and the legislation of other jurisdictions, the Administration considered the proposed penalty levels appropriate. In respect of the obligations of third-party service providers, the regulating authorities would refer to the practices in other jurisdictions and provide guidelines on possible reasonable excuses such as "due diligence" and "reasonable endeavour" in CoP, so as to provide reference for designated operators in the formulation and performance of contracts when engaging third-party service providers. The Administration emphasized that if the relevant violation involved infringement of other criminal legislation (e.g. fraud-related crimes), the personnel involved could be held criminally liable on a personal basis.

14. There were views that the authorities might consider establishing a compensation mechanism under the proposed legislation to **require designated operators to compensate affected individuals following the occurrence of computer-system security incidents.** The Administration advised that, as at present, affected individuals might seek compensation through civil proceedings on a case-by-case basis.

Regulating authorities and appeal mechanism

15. Members noted that under the legislative proposals, a Commissioner to be appointed by the Chief Executive and designated authorities of some sectors[4] would act as regulating authorities. The Administration also proposed the establishment of a Commissioner's office under the Security Bureau to implement the legislative regime. Members sought the Administration's elaboration on the proposed **staffing establishment of the Commissioner's office**. The Administration advised that the Commissioner's office would be headed by a Commissioner (at D3 or D4 level) to be appointed by the Chief Executive, and supported by two Deputy Commissioners (at D1 level). The Commissioner's office would have about 40 to 50 non-directorate staff, including staff seconded from DPO and the Technology Crime Division of the Hong Kong Police Force, as well as legal professionals and policy formulation officers.

16. Members noted that as some of the essential services sectors proposed for regulation were already subject to comprehensive regulation by other statutory sectoral regulators, individual sectoral regulators would, under the legislative proposals, be designated as designated authorities responsible for supervising compliance with the obligations relating to organization and prevention of threats and incidents by designated operators under their regulation. The designated authorities proposed by the Administration at this stage were the Monetary Authority (with banking and

[4] See paragraph 16 below.

financial services sector being the corresponding sector) and the Communications Authority (with telecommunications and broadcasting services sector being the corresponding sector). The Commissioner would have overall responsibility for supervising compliance with the obligations relating to incident reporting and response by all designated operators. Members sought clarification from the Administration on whether the failure of a designated operator regulated by a designated authority to comply with its obligations relating to organization and prevention of threats and incidents would be dealt with solely under the penalty mechanism of the designated authority. The Administration advised that the basic principle was that the case would be dealt with in accordance with the mechanism of the designated authority. For example, depending on the circumstances, the designated authority could revoke the licence it had issued.

17. There were concerns that **some statutory sectoral regulators** (such as the Insurance Authority, which regulated the insurance industry (fallen under the financial services sector under the proposed Ordinance)) **were not designated as designated authorities under the proposed legislation**. The Administration advised that it would take into account the development in the relevant industries and regulatory regimes and conduct review when appropriate.

18. With regard to the appeal board to be established under the legislative proposals to handle appeals lodged by designated operators against certain decisions of the regulating authorities, members expressed concerns about the **composition of the appeal board** and measures to **avoid conflicts of interest among its members**, in view of the limited supply of computer security professionals in the market. The Administration advised that under the proposed appeal mechanism, the Chief Executive would appoint a chairman and two vice-chairmen, as well as at least 8 to 10 members, including legal professionals, information technology professionals and other members of the community. The appeal board would act in accordance with the established practice in dealing with conflicts of interest.

Relevant papers

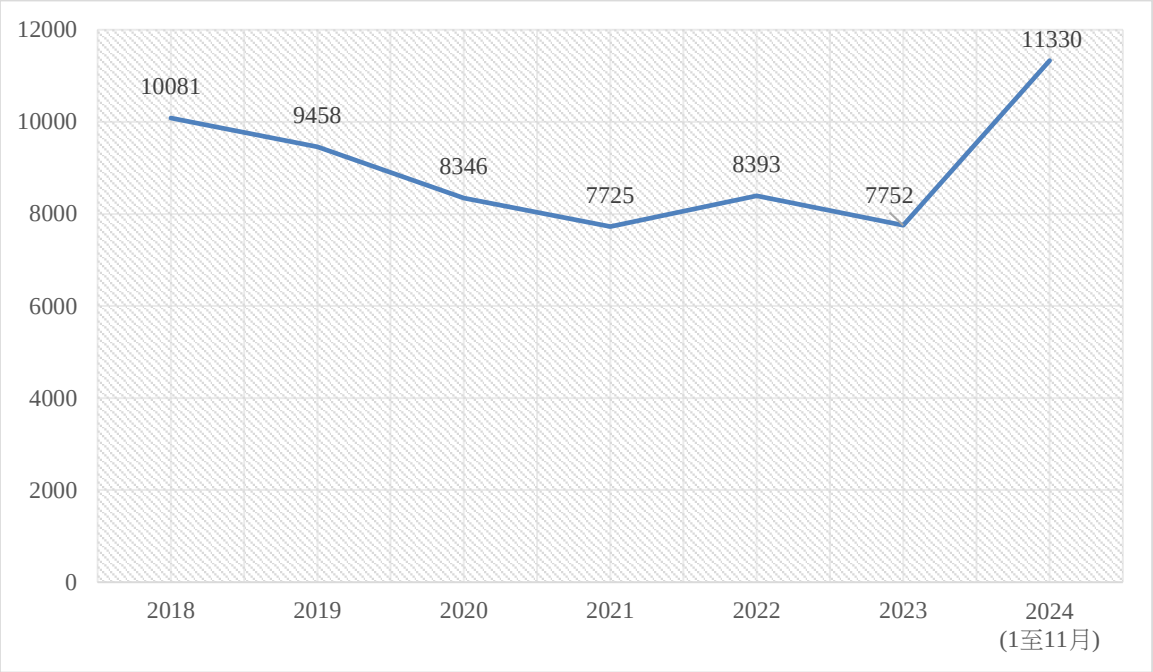
19. A list of the relevant papers on the LegCo's website is in **Appendix 2**.

Council Business Divisions
Legislative Council Secretariat
3 January 2025

Appendix 1

Statistics of security incidents reported to the Hong Kong Computer Emergency Response Team Coordination Centre from January 2018 to November 2024

Total numbers of incidents received[1]



Source: The Hong Kong Computer Emergency Response Team Coordination Centre (website: https://www.hkcert.org/statistic)

---

[1] For the period between 2018 and November 2024, the most prevalent types of security incidents received by the Hong Kong Computer Emergency Response Team Coordination Centre:

(a) Botnet (A botnet is composed of a group of zombie computers, most of which are personal computers infected by malicious software. Once infected, the malicious software usually hides itself and stealthily connects to the Command & Control Server to get instructions from the hackers and launch attacks);

(b) Malware (as a general terminology and some common types of malware are viruses, ransomware, worms, Trojan horse, spyware and adware); and

(c) Phishing (i.e. the spoofing of a legitimate website for fraudulent purposes).

Appendix 2

Protection of Critical Infrastructures (Computer Systems) Bill

List of relevant papers

Committee	Date of meeting	Paper
Panel on Security	25 October 2021	Agenda Item II: Briefing by the Secretary for Security on the Chief Executive's 2021 Policy Address Minutes of policy briefing-cum-meeting
	8 February 2022	Agenda Item III: Briefing by the Secretary for Security on the Chief Executive's 2021 Policy Address Minutes of policy briefing-cum-meeting
	31 October 2022	Agenda Item IV: Briefing by the Secretary for Security on the Chief Executive's 2022 Policy Address Minutes of policy briefing-cum-meeting
	13 November 2023	Agenda Item III: Briefing by the Secretary for Security on the Chief Executive's 2023 Policy Address Minutes of policy briefing
	2 July 2024	Agenda Item III: Proposed legislative framework to enhance protection of the computer systems of critical infrastructure Minutes of meeting
	2 October 2024*	Administration's information paper on Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructures

* Date of issue

Council Business Divisions
Legislative Council Secretariat
3 January 2025