立法會
Legislative Council

LC Paper No. CB(2)930/2024(04)

Ref : CB2/PL/SE

Panel on Security

Meeting on 2 July 2024

Background brief on enhancing the protection of cybersecurity of critical infrastructure

Purpose

This paper provides background information and gives an account of Members' past discussion on matters relating to the Administration's legislation on cybersecurity obligations of operators of critical infrastructure ("CI") in Hong Kong.

Background

2. Cybersecurity is **one of the 20 major security fields under the holistic view of national security** introduced by President Xi Jinping. According to the Administration, cybersecurity refers to a state in which necessary measures are taken to prevent cyber-attacks, network intrusions, cyber interference, cyber sabotage, unlawful use of network, and cybersecurity incidents, thereby ensuring stable and reliable operation of networks, and the capacity to maintain the integrity, confidentiality and availability of network data. The Mainland has enacted the Cybersecurity Law in 2016.

Protecting cybersecurity in Hong Kong

3. Cybersecurity threats are increasingly commonplace. Against the above, the Administration has all along been making efforts to build up the capability of public and private organizations to safeguard their systems and enhance security of their networks and data against cyber-attacks. That said, the number of cybersecurity incidents has continued to rise in recent years, with a total of 9 017 cybersecurity incidents reported to the Hong Kong Computer Emergency

Response Team Coordination Centre ("HKCERT")[1] from June 2023 to May 2024. In respect of government information systems and data, the Administration has adopted multi-pronged security measures and implementation mechanisms on data security risk management, covering data protection, audit and risk assessment, incident handling and response, education and training, etc. In April 2000, the Information Security Management Committee, core members of which comprising representatives of the Office of the Government Chief Information Officer ("OGCIO") and the Security Bureau, was established to oversee information technology ("IT") security within the whole Government.[2]

Protection of security of critical infrastructure in Hong Kong

4. The responsibility of protecting the physical security of CI is vested with the Critical Infrastructure Security Coordination Centre ("CISCC") established by the Hong Kong Police Force ("HKPF") in 2011. Through public-private partnership, CISCC aims at strengthening the self-protection capabilities of CI in Hong Kong. Meanwhile, to safeguard CI in the sectors of government, banking and finance, transportation, communications and public utilities from cybercrime[3], the Cyber Security Centre ("CSC") under the Cyber Security and Technology Crime Bureau ("CSTCB") of HKPF conducts timely cyber threat audits and analyses to prevent and detect cyberattacks against CI. Both CISCC and CSC provide round-the-clock support to local CI.

Members' views and concerns

Safeguarding important facilities and infrastructure in Hong Kong

5. Referring to the cyber-attacks targeted at key infrastructure abroad, Members sought the Administration's elaboration on **the HKPF's work to**

---

1 HKCERT under the Hong Kong Productivity Council is the centralized contact on the reporting of and response to computer and network security incidents for local businesses and Internet users. It also gathers and disseminates information on security related issues and provides advice on preventive measures against relevant threats.

2 The Committee meets regularly to: (a) review and endorse changes to the government IT security related regulations, policies and guidelines; (b) define specific roles and responsibilities relating to IT security; and (c) provide guidance and assistance to bureau and departments in the enforcement of IT security related regulations, policies, and guidelines through the IT Security Working Group (i.e. the executive arm of the Committee).

3 According to HKPF, offences related to conducts in the cyber world under the existing legislation include, among others, (a) section 27A of the Telecommunications Ordinance (Cap. 106) prohibiting unauthorized access to computer by telecommunications, and (b) sections 60 and 161 of the Crimes Ordinance (Cap. 200) prohibiting destroying or damaging property and access to computer with criminal or dishonest intent respectively.

ensure the security of CI, especially the objectives of and agencies involved in the related drills conducted by HKPF. The Administration advised that CSTCB of HKPF had been working closely with CI operators in various sectors so as to enhance their response capability against cybersecurity incidents and cyber-attacks. Efforts being made included conducting cybersecurity exercises with CI operators to foster cybersecurity collaboration between HKPF and CI operators, as well as sharing information on cyber threats and relevant preventive and responding actions in order to enhance CI operators' awareness of prevention and preparedness, as well as their overall defensive capabilities against cyber-attacks.

6. Members sought **the Administration's elaboration on the preparatory work to formulate legislative proposals on the cybersecurity obligations of operators of CI**, including the reference made to the relevant legislation of other places (say Mainland's Regulation for Safe Protection of Critical Information Infrastructure), the obligations to be imposed on the board of directors of the operators of CI, as well as the views of the industries on the proposed legislative framework. Members also enquired about whether a dedicated agency would be set up to perform duties relating to protection of cybersecurity of CI.

7. The Administration advised that to take the exercise forward, it had looked into relevant regulatory frameworks in the Mainland, Macau, Singapore, the United Kingdom, Australia and the United States. Pursuant to its exchange of views with the trade, the relevant industries were in general supportive to the proposed legislation, and many major operators of CI had already put in place preventive management systems to guard their infrastructure against cyber-attacks. Subject to the finalized provisions of the legislative proposals, a dedicated office was proposed to be set up for implementing the legislation, and arrangements would be made in accordance with the Administration's established procedures on manpower and set-up required for the office in due course, so as to carry out the relevant work on the protection of cybersecurity of CI after the enactment of the legislation.

<u>Defending cyber-attacks and responding to cybersecurity incidents</u>

8. Members expressed grave concern about the recent cyber-attacks targeted at public organizations leading to data breaches and sought **the Administration's elaboration on the root cause of these incidents**. They further enquired about the number of systems (say websites, applications and hosts) of bureaux and departments ("B/Ds") and public organizations which had been subject to ransomware attacks, including those not being disclosed to the public, as well as whether these attacked systems were covered by continuous security assessment and improvement programmes.

9. According to the Administration, it did not maintain statistics of cyber-attacks targeted at public organizations. In the meantime, according to the Government's information security incident response mechanism, all B/Ds were required to report information security incidents to OGCIO upon their occurrence and OGCIO, through its Government Computer Emergency Response Team Hong Kong ("GovCERT.HK"), had handled nine reported security incidents relating to Government installations in 2023, with the top three types of reported incidents being loss of mobile devices or removable media containing classified data (accounting for 23% of the incidents so reported), as well as ransomware and compromise of information systems or data assets, both of which represented 22% of these reported incidents.[4]

10. Members expressed concerns about the **governance structure in respect of the cybersecurity area in the Government and public organizations**, including **whether OGCIO has a role to play in the cybersecurity area of public organizations**, **whether the set of Government IT Security Policy and Guidelines ("Policy and Guidelines")** devised and regularly updated by OGCIO **were applicable to public organizations**, as well as whether reference would be made to the related governance structure in Singapore by establishing a Public Sector Data Security Review Committee and a data bureau.

11. The Administration advised that it had put forth a multi-layered system covering assessment, monitoring, risk management and contingency to ensure information security of B/Ds which were required to, based on a risk-based approach, continuously identify security risks of their information systems. Such requirements included the regular conduct of independent information security risk assessments and review of current security measures for keeping relevant measures abreast of the times and ensuring their effectiveness in tackling the latest cyber risks. Meanwhile, whereas the Policy and Guidelines devised and regularly updated by OGCIO were intended only for compliance by B/Ds, OGCIO had uploaded the Policy and Guidelines to its website for reference by other organizations.[5] Public organizations could formulate and adopt computer systems, IT governance policies and cybersecurity defense measures which best suit their own operation, and enhancement to their IT infrastructure would be carried out based on actual circumstances and the latest technology development.

---

[4] Statistics on information security incidents in the Government are available on the Government's Public Sector Information Portal for public access and related figures are updated by OGCIO on a monthly basis.

[5] The Policy and Guidelines are accessible at https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/.

12. Referring to the pivotal role played by HKPF, Members enquired about the updates in contingency plans developed by HKPF to **address, among others, increasing cyber-attacks**. The Administration advised that to combat new types of cyber-attacks, HKPF had put forth a series of related measures including enhancing public-private partnerships and conducting regular cybersecurity exercises, thereby preventing illegal acts that endanger national security and advocate terrorism through the Internet. That apart, GovCERT.HK of OGCIO and CSTCB had jointly hosted the Inter-departmental Cyber Security Drill since 2017, with a view to enhancing the cybersecurity awareness and overall response capabilities of B/Ds. The above Drill was last held on 25 April 2024 and attended by over 250 government officers from 70 B/Ds.

Relevant papers

13. A list of the relevant papers on the Legislative Council's website is in the **Appendix**.

Council Business Division 2
Legislative Council Secretariat
28 June 2024

Appendix

List of relevant papers on enhancing the protection of cybersecurity of critical infrastructure

Committee	Date of meeting	Paper
Panel on Security	8 February 2022	Agenda item III: Briefing by the Secretary for Security on the Chief Executive's 2021 Policy Address Minutes
	31 October 2022	Agenda item IV: Briefing by the Secretary for Security on the Chief Executive's 2022 Policy Address Minutes
Finance Committee	12 April 2023	Administration's replies to Members' initial written questions raised in the examination of the Estimates of Expenditure 2023-2024 (Reply Serial Nos.: SB011 and SB065)
Panel on Security	13 November 2023	Agenda item III: Briefing by the Secretary for Security on the Chief Executive's 2023 Policy Address Minutes
Finance Committee	18 April 2024	Administration's replies to Members' initial written questions raised in the examination of the Estimates of Expenditure 2024-2025 (Reply Serial Nos.: SB019 and SB062)

Council meeting	Paper
18 October 2023	Question 17: Enhancing cybersecurity
22 November 2023	Question 11: Cybersecurity of government departments and other public organizations
29 May 2024	Question 18: Cybersecurity of government departments and other public organizations

Council Business Division 2
Legislative Council Secretariat
28 June 2024