立法會
Legislative Council

LC Paper No. CB(2)1189/2024(03)

Ref.: CB/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 14 October 2024

Background brief on safeguarding and promoting information security

Purpose

This paper provides background information on the Administration's measures in safeguarding and promoting information security. It also gives a brief account of the views and concerns expressed by Members during discussions on related subjects at the meetings of the Panel on Information Technology and Broadcasting ("the Panel") and the Subcommittee on Matters Relating to the Development of Smart City in recent years.

Background

2. The objectives of the Administration's information security programmes are to:

(a) formulate and implement information security policies and guidelines for compliance and reference by bureaux and departments ("B/Ds");

(b) ensure that all the Administration's information technology ("IT") infrastructure, systems and information are secure and resilient; and

(c) promote and enhance the awareness of information security and cyber risks among organizations and members of the public.

3. The Administration has launched dedicated programmes under the following three main areas:

(a) information security in Government;

(b) information security initiatives in the community; and

(c) professional training and public awareness.

Information security in Government

Strengthening information and cyber security of the Government and public organizations

4. In December 2023, the Administration published the **Policy Statement on Facilitating Data Flow and Safeguarding Data Security in Hong Kong** to set out the Government's management principles and strategies on data flow and data security, including formulating rules relating to usage and safety to protect its IT systems and data security, as well as **studying amendments to the Personal Data (Privacy) Ordinance (Cap. 486) and exploring further enhancement of the Copyright Ordinance (Cap. 528)**, with the objectives of strengthening protection for personal data and artificial intelligence technology development.

5. To ensure the smooth implementation and operation of government IT systems, the Office of the Government Chief Information Officer ("OGCIO")[1] introduced a series of new measures in February 2024, including requiring B/Ds to **arrange additional independent cyber security tests for large-scale and high-risk IT projects before launch**, to detect and patch relevant systems' vulnerabilities at an early stage and assess the detection and resilience capabilities of the systems in response to cyber attacks. The Administration will take the lead in **organizing cyber security attack and defence drills** in the second half of 2024 to test and strengthen the information systems security of government departments and public bodies, by leveraging the capabilities and experiences of Mainland organizations specialized in attack and defence drills.

---

[1] OGCIO and the Efficiency Office merged to form the Digital Policy Office ("DPO") in July 2024. DPO is responsible for formulating policies on digital government, data governance and IT.

6. Furthermore, OGCIO has formulated and updated from time to time the Government Information Technology Security Policy and Guidelines ("the Policy and Guidelines"), which covers the information security management framework, policies and measures for B/Ds to comply with and adopt, and for reference by the industry (including both public and private organizations). The revised Policy and Guidelines promulgated by OGCIO in April 2024 strengthened security control measures in various areas including the incident reporting mechanism. To effectively safeguard the Government's information systems and data security, **classified protection of IT security** was also **enhanced** to mandate all B/Ds to adopt a risk-based approach to assess the classifications of their information systems and implement corresponding tiered security control measures according to the classifications.

Information security compliance audits

7. OGCIO has launched independent information security compliance audits regularly for B/Ds to ensure their strict compliance with government security requirements. OGCIO has completed the compliance audits in 2022-2023 and provided recommendations to assist B/Ds in the continuous optimization of the security management system. The Administration plans to start a new round of information security compliance audits in the second half of 2024.

Computer system security of critical infrastructures

8. Critical infrastructures ("CIs") refer to the facilities that are necessary for the maintenance of normal functioning of the Hong Kong society and the normal life of the people, such as banks, financial institutions, telecommunications service providers, electricity supply facilities, railway systems, etc. In the event that the computer systems of CIs are being disrupted or sabotaged, the normal functioning of society will be seriously affected. The Administration announced in July 2024 the proposed legislative framework for **enhancing protection of computer systems of CIs**. The proposed legislative framework seeks to provide for the statutory obligations to be fulfilled by CI operators ("CIOs") so that they would take appropriate measures to strengthen the security of the relevant computer systems and minimize the chance of essential services being disrupted or compromised due to cyber attacks, thereby enhancing the overall computer system security in Hong Kong. A relevant bill is expected to be introduced into the Legislative Council by end-2024.

Information security initiatives in the community

Monitoring, preventing and responding to cyber threats and attacks

9. The Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT")[2] coordinates computer security incident responses, monitors and disseminates security alerts, as well as promotes information security awareness to local enterprises and the public. HKCERT also collaborates with Internet services providers to promote information security best practices to make Hong Kong a safe Internet hub.

10. The Government Computer Emergency Response Team Hong Kong ("GovCERT")[3] maintains close liaison with other regional CERTs through the CERT Coordination Centre, the Forum of Incident Response and Security Teams, and the Asia Pacific Computer Emergency Response Team ("APCERT") to facilitate timely sharing of information on security threats, vulnerabilities and security incidents. To foster collaborative exchanges and sharing of information security intelligence, GovCERT actively participates in relevant activities organized by different organizations, including the joint annual incident response drill organized by APCERT.

Enhancing the capability of Hong Kong enterprises (in particular small and medium enterprises) in responding to cyber attacks

11. To assist small and medium enterprises ("SMEs") in coping with potential information security risks with limited resources, the Hong Kong Internet Registration Corporation Limited ("HKIRC") started to provide free scanning services for SME websites as early as 2019, including checking whether the websites have security vulnerabilities, as well as providing scanning reports and recommendations. HKCERT also launched

---

[2] Established by the Government in 2001, HKCERT is now managed by the Hong Kong Productivity Council with the missions of facilitating information dissemination on security incidents among local enterprises and Internet users, providing advices on preventive measures against security threats, and promoting information security awareness of the public.

[3] Established under OGCIO in April 2015, GovCERT is dedicated to coordinating information and cyber security incidents for the Government. GovCERT is the coordination centre for government IT administrators and departmental Information Security Incident Response Teams on computer emergency response and incident handling. GovCERT works closely with HKCERT to share information on security threats and vulnerabilities, and provide recommendations to the public/private sectors and individuals in protecting their information systems and digital assets.

the Check Your Cyber Security Readiness online self-assessment tools in September 2021 to provide SMEs with a better understanding of their cyber security status and provide recommendations to assist them in uplifting their overall information security capability. Meanwhile, through the Partnership Programme for Cyber Security Information Sharing, OGCIO has also partnered with HKIRC to promote the exchange of cyber security information among public and private organizations. In addition, under various initiatives such as the Technology Voucher Programme, the Administration has been providing financial support to enterprises for the enhancement of their capability in maintaining information security.

Public awareness of cyber security

12. The Administration provides information security advice to the public through various channels, including radio, social media, websites, etc. For instance, the Hong Kong Police Force ("HKPF") comprehensively disseminates anti-scam messages by organizing Anti-Deception Month and launching the Anti-Deception Coordination Centre One-Stop Platform website. Furthermore, OGCIO has continued to organize the annual Build a Secure Cyberspace information security promotional campaign in conjunction with HKPF and HKCERT to strengthen the understanding of organizations and the general public on cyber security and national security. They were reminded to behave prudently in the cyber world and jointly maintain cyber security.

13. To further combat telephone and SMS frauds, the Office of the Communications Authority introduced the **SMS Sender Registration Scheme** ("the Scheme") in late December 2023. The Scheme was **first implemented in the telecommunications sector** to help members of the public verify the identities of SMS senders. Under the Scheme, all participating companies or organizations will use Registered SMS Sender IDs with the prefix "#" when they send SMS messages to local subscribers of mobile services.

<u>Manpower development in information security</u>

14. The Administration continues to implement the Technology Talent Admission Scheme ("TechTAS")[4] and streamline the admission procedure for technology talent (including that in cyber security) undertaking research and development ("R&D") work. This has expedited

---

[4] TechTAS was launched in 2018 to provide a fast-track arrangement for admitting overseas and Mainland technology talent. Successful companies would be given quotas for bringing in such people for undertaking R&D work.

the admission of cyber security technology talent from different parts of the world. In December 2022, the Administration launched various enhancement measures, including lifting the local employment requirement, extending the quota validity period to two years and expanding the coverage to more emerging technology areas.

Major views and concerns expressed by Members

15. The major views and concerns expressed by Members are summarized in the ensuing paragraphs.

Information security policies of the Administration

16. Members noted that in the wake of Cyberport's cyber security incident in August 2023, OGCIO had reminded all **government departments** to review their information security systems and **enhance their cyber security defence**. Members enquired about the **progress** of the relevant work and whether OGCIO would set up a cyber security response team to handle emergencies, as well as review and update the Policy and Guidelines, and whether it would require other public organizations to follow suit so as to assist them in formulating the relevant measures.

17. The Administration advised that it would proactively follow up cyber security incidents of the Government and public organizations. As most government systems were managed centrally on the Government's private cloud platform with access to the Internet through the Central Internet Gateway, security arrangements could be made in a more coordinated manner. The Administration had adopted multi-layered cyber security technologies, firewalls, intrusion detection and response systems, etc. to monitor system traffic, conduct analysis and issue alerts. OGCIO had also required each department to set up a computer emergency response team such that OGCIO would be notified immediately in case of an incident. The Administration would step up attack and defence drills to examine the vulnerabilities of departmental systems and work closely with the Cyber Security and Technology Crime Bureau of HKPF to assess the cyber security situation on a regular basis. The Administration would step up the collaborative efforts with the industry in the future to safeguard the overall cyber security of Hong Kong.

18. Regarding the Policy and Guidelines relating to IT security, the Administration advised that it would be updated and uploaded on a regular basis for reference by all public and private organizations, and individual

organizations could adopt the principles and measures recommended in the Policy and Guidelines for managing security risks as appropriate. In this regard, Members called on the Administration to **consolidate different information security guidelines** with a view to **providing more comprehensive guidelines** to organizations. To raise the awareness of information security risks of all B/Ds, OGCIO had regularly reminded B/Ds to adopt effective security measures to protect government information systems and data.

Strategies to tackle cyber security threats

19. In view of the increasing severity of global cyber attacks, Members held that the Administration should **formulate all-round information security strategies** to tackle cyber security threats on various fronts. Members also suggested that the Administration should adopt the Mainland-developed Harmony (鴻蒙) operating system in government computer systems to **reduce reliance on foreign technologies**.

20. The Administration advised that it would maintain liaison with global leading computer emergency incident response organizations and computer emergency response teams for the exchange of latest cyber security information. OGCIO had made collaborative efforts with HKCERT and HKIRC through the Partnership Programme for Cyber Security Information Sharing to enhance the capability of Hong Kong enterprises (in particular SMEs) in dealing with various types of cyber attacks, including providing free scanning service for SME websites with ".hk" domains, publishing the Information Security Incident Guidelines, and developing training materials for SME employees. As regards the security protection of government information systems, the Administration had reminded B/Ds to procure information and communication technology products from diverse sources so as to reduce the security risk and reliance on single products or brands.

Computer system security of critical infrastructures

21. Members noted that the Administration had announced the proposed legislative framework for strengthening the protection of computer system security of CIs, with the aim of defining the statutory obligations of **CIOs (government departments to be excluded)**, including the establishment of good preventive management system to ensure the secure operation of their information systems and networks. Members enquired about the Administration's **measures to ensure the cyber security of government departments** if they were to be excluded from the proposed legislation.

22. The Administration advised that for essential services operated by the Government (e.g. water supply, drainage, emergency relief, etc.), government departments should adhere to the comprehensive and stringent Policy and Guidelines with regular review and updating, taking into account the latest international standards and industry best practices, to ensure the security of government information systems. As the level of requirements in the Policy and Guidelines was comparable to the statutory requirements for CIOs under the proposed legislation, the Administration proposed to continue regulating government departments through the existing administrative approach without netting them into the scope of regulation of the proposed legislation.

Helping small and medium enterprises respond to cyber security risks

23. Members enquired about the Administration's measures to **help SMEs respond to cyber security risks**. In this regard, they suggested that the Administration should **collaborate with sizeable organizations or trade associations** to provide assistance to the industry. The Administration advised that the Government would step up the collaborative efforts with the industry and support the industry in addressing cyber security risks on various fronts, including offering free website security detection services for SMEs, setting up staff training platforms and formulating Practice Guides on Data Centre Security in consultation with the industry, thereby enhancing the awareness and capability of the industry and the general public in safeguarding cyber security. The Administration would also collaborate with HKIRC to step up promotion, publicity and training efforts to raise cyber security awareness, together with the provision of "Healthy Web" service and support on information security incident responses.

Cyber deception

24. Members were concerned about the significant increase in the number of online deception cases and the amount of monetary loss involved. They asked the Administration to enhance public education and publicity so as to **raise public awareness of online fraud and cyber security**. The Administration advised that HKPF established the Anti-Deception Coordination Centre in 2017 to reinforce the efforts in combating against deception. In addition, the Anti-Deception Coordination Centre One-stop Platform website had been launched to raise the public's awareness of deception activities. HKPF would also closely monitor potential criminal

activities online and conduct targeted searches on public online platforms for pertinent criminal information.

Information security talent

25. Concerned about the lack of talent in Hong Kong with specialized knowledge in information security, Members suggested that such personnel should be trained by the Administration for undertaking information security projects of various departments and public organizations and enhancing protection in this regard. The Administration advised that while the training of information security experts would need to be strengthened continuously, efforts would also be made to attract overseas and local cyber security experts and organizations to support the relevant work in Hong Kong.

26. Members asked how the Administration would **nurture more information security talents**. The Administration advised that it would strengthen exchanges with the industry by organizing regular sharing sessions or technical exchange activities, such as inviting outstanding Mainland companies in cyber security to Hong Kong for sharing. These events would bring about additional demand from Hong Kong enterprises for cyber security, with a view to attracting Mainland enterprises and talents to set up in Hong Kong and strengthening Hong Kong's pool of cyber security talents. Apart from attracting cyber security technology talent from different parts of the world, the Administration encouraged local tertiary institutions and technology training providers to provide professional training courses for IT practitioners to build up professional knowledge and skills in information security.

Council motions and questions

27. At the Council meeting of 29 November 2023, Members passed a motion on "Combating cyber fraud crimes on all fronts", urging the Government to enhance the existing measures for combating cyber fraud, including comprehensively examining the cyber security risks in Hong Kong, stepping up the protection measures for cyber systems, assisting SMEs in raising their cyber security level, etc. The wording of the motion is hyperlinked in the **Appendix**.

28. Members have raised questions relating to cyber security, combating cyber fraud, protection of personal data privacy, etc. at various Council meetings. The relevant hyperlinks are in the **Appendix**.

Latest development

29. The Administration will report to the Panel on 14 October 2024 on the latest situation of information security in Hong Kong, as well as the Government's work on safeguarding and promoting information security.

Relevant papers

30. A list of relevant papers is set out in the **Appendix**.

Council Business Divisions
Legislative Council Secretariat
9 October 2024

Appendix

Work related to safeguarding and promoting information security

List of relevant papers

Committee	Date of meeting	Paper
Panel on Information Technology and Broadcasting	19 April 2022	Agenda Item IV: Update on information security Minutes of meeting
	12 December 2023	Agenda Item III: Facilitating data flow and safeguarding data security Minutes of meeting
	8 April 2024	Agenda Item V: Cyberport's cybersecurity incident Minutes of meeting
Subcommittee on Matters Relating to the Development of Smart City	12 July 2024	Agenda Item I: Update on Smart City Development of Hong Kong Minutes of meeting
Special meetings of the Finance Committee to examine the Estimates of Expenditure 2024-2025	19 April 2024	Written replies to initial questions raised by Members in examining the Estimates of Expenditure 2024-2025 (Reply Serial Nos.: ITIB019, 159, 205, 229, 237, 242 and 251) Verbatim record

Council meeting	Paper
25 May 2022	Question 1: Strengthening information security
26 October 2022	Question 2: Combating online and telephone frauds
10 May 2023	Question 10: Protecting personal data when developing and using artificial intelligence

Council meeting	Paper
5 July 2023	Question 6: Building a strong digital security barrier
5 July 2023	Question 13: Deception cases on social media platforms
18 October 2023	Question 17: Enhancing cyber security
15 November 2023	Question 9: Data governance system
15 November 2023	Question 14: Combating online and telephone frauds
22 November 2023	Question 11: Cybersecurity of government departments and other public organizations
29 November 2023	Members' motion: Combating cyber fraud crimes on all fronts Progress report
17 January 2024	Question 3: Ensuring the normal operation of government electronic systems
29 May 2024	Question 6: Protection of personal data privacy
29 May 2024	Question 18: Cybersecurity of government departments and other public organizations