立法會
Legislative Council

LC Paper No. CB(2)1860/2025(02)

Ref: CB2/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 13 October 2025

Background brief on safeguarding information security

Purpose

This paper summarizes Members' past discussions on the Government's various measures to safeguard information security since the Seventh Legislative Council ("LegCo").

Background

2. The Administration adopted a multi-pronged approach to enhance information security in Hong Kong, which included: (a) **formulating and implementing information security policies and guidelines** for compliance and reference by bureaux and departments ("B/Ds"); (b) working with stakeholders such as the Hong Kong Internet Registration Corporation Limited ("HKIRC") and the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") to provide the general public with relevant information and support, thereby **enhancing community awareness and defensive capability in terms of cybersecurity**; (c) **coordinating the handling of information and cybersecurity incidents within the Government** through the Government Computer Emergency Response Team Hong Kong; and (d) encouraging tertiary institutions and other relevant bodies to provide more training programmes on information and cybersecurity, as well as implementing the Technology Talent Admission Scheme, with a view to **improving the training and admission of more related technology talent**.

3. Meanwhile, LegCo passed the **Protection of Critical Infrastructures (Computer Systems) Bill** ("the Bill") on 19 March 2025. **The Bill imposed statutory obligations on designated "operators of critical infrastructures"** ("CI Operators"), ensuring that CI Operators had put in place appropriate measures to protect their computer systems and minimize the chance of essential services being disrupted or compromised due to cyberattacks, thereby enhancing the overall computer system security in Hong Kong.

Current local cybersecurity situation

4. According to the information provided by the Administration and HKCERT, HKCERT handled a total of 12 536 **security incidents** in 2024, representing a **62% increase** compared with 2023. The Police recorded 33 903 **technology crimes** in total, representing a **0.6% decrease** compared with 2023, and including 112 destructive cyberattacks. The figures for security incidents and technology crimes recorded in Hong Kong in 2024 are set out below:

	Types	**Number of cases**		**Year-on-year comparison**
		Number	Percentage	
Security incident	Total:	12 536	100%	+62%
	Major types: (a) Phishing (b) Botnet (c) Malware	 7 811 2 889 964	 62% 23% 8%	 +108% -3% +484%
Technology crime	Total:	33 903	100%	-0.6%
	Major types: (a) Online deception (b) Misuse of computer (c) Internet blackmail	 27 485 3 055 2 559	 81% 9% 8%	 +0.6% -12% +5.4%

Sources : *(a) Security incidents reported to HKCERT in 2024, available at the website of HKCERT*

(b) Administration's reply to the relevant written question raised by Legislative Council Members in examining the Estimates of Expenditure 2025-2026

5. In June 2025, the Police released the Cybersecurity Report 2024, which highlighted the **three recurring system vulnerabilities in cybersecurity incidents** in Hong Kong. They included **inadequate access**

control and configuration, outdated and unpatched systems, and the **lack of effective threat detection mechanism**. The report also revealed that **55%** of the city's critical infrastructure **had experienced cyberattacks or cybersecurity incidents in 2024**. The most common types of cyberattacks involved were fraudulent emails, fraudulent websites, and denial-of-service or distributed denial-of-service attacks.

Members' views and concerns

Enhancing information security of the Government and public organizations

6. Members expressed concern about the cybersecurity incidents involving government departments or public organizations in recent years. Members were of the view that the Administration should **examine the implementation of the relevant information security guidelines by B/Ds** to gauge the effectiveness of their work in safeguarding information security, and that the heads of various government departments and the heads of information technology ("IT") security of such departments should be held accountable for the security work of the computer systems in their departments, and disciplinary actions should be taken against officers involved in cases of human negligence or non-compliance.

7. The Administration advised that the Digital Policy Office ("DPO") would proactively inspect government information systems and launch information security compliance audits for B/Ds. B/Ds were required to safeguard the security of IT systems under their purview, including that the heads of B/Ds would handle cases involving suspected violation of relevant regulations or engagement in illegal acts by their personnel or contracted service providers in accordance with the established procedures. Various B/Ds and relevant public organizations were also requested to adopt enhancement measures, such as conducting tests for large-scale and high-risk IT projects, and enhance their key supervisory role over government IT projects.

8. Noting that **the Bill was not applicable to the Government**, Members were concerned about **how the security of the computer systems in B/Ds which were crucial to the normal functioning of the society could be ensured**. The Administration advised that B/Ds were required to strictly comply with the Government Security Regulations and the Government Information Technology Security Policy and Guidelines ("Policy and Guidelines"), which would be reviewed and updated regularly with reference to the latest national and international standards, as well as industry best practices. The Administration considered it appropriate to continue with the established practice of adopting an administrative approach to ensure

compliance by B/Ds with the requirements without including them in the Bill for regulation.

9. Some Members suggested that the Administration should **review and update the Policy and Guidelines, such that public organizations would be required to adhere to them** when formulating relevant measures. It was also suggested that **different information security guidelines should be consolidated** to provide public and private organizations with more comprehensive guidelines. The Administration advised that the Policy and Guidelines would be updated and uploaded onto the Internet on a regular basis for reference by all public and private organizations.

10. Members enquired whether the Administration would **formulate contingency plans** and **organize cybersecurity attack and defence drills** to **enhance the response capabilities of B/Ds against information security incidents**. The Administration advised that under the existing information security incident handling mechanism, B/Ds and relevant public organizations were required to conduct an incident impact assessment upon the occurrence of information security incidents, report the incidents to the respective bureaux and DPO, and notify relevant regulatory authorities depending on the nature of the incidents. B/Ds were also required to follow the requirements of the Policy and Guidelines to set up Information Security Incident Response Teams and formulate relevant response plans, so as to ensure the response in the event of a security incident was appropriate and effective. The Administration also indicated that cybersecurity attack and defence drills would be organized on a regular basis.

11. Members were concerned about the measures put in place by the Administration to **ensure the cybersecurity of the use of personal webmail, public cloud storage and web-version of instant messaging services by civil servants and other government employees**. The Administration advised that DPO updated the Policy and Guidelines in April 2024, setting out the security guidelines for the use of desktop computers connected to the government internal network systems, which included the requirement for staff of B/Ds to obtain approval from their management before using the aforementioned services on desktop computers connected to the government internal network. Meanwhile, B/Ds should critically review the necessity of the access to such services by their staff on a regular basis and revoke the relevant access right when no longer required.

Helping small and medium enterprises respond to cybersecurity risks

12. Members enquired about the Administration's measures to **help small and medium enterprises** ("SMEs") **respond to cybersecurity 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 it would support the industry in addressing cybersecurity 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 cybersecurity. The Administration would also collaborate with HKIRC to step up promotion, publicity and training efforts to raise cybersecurity awareness, together with the provision of "Healthy Web" service and support on information security incident responses.

Enhancing the protection against unauthorized access to online service accounts

13. Members were concerned about the upsurge in the number of cases of unauthorized access to online service accounts in recent years and urged the Administration to **step up efforts in preventing and combating fraudulent activities**, particularly **crimes with the use of technologies such as deepfake technology and generative artificial intelligence** ("AI"). There were suggestions that the Administration should strengthen cooperation with operators of social media platforms in blocking online fraudulent advertisements, and that considerations should be given to introducing legislation to stipulate the responsibilities of the relevant operators in handling information such as fraudulent web pages or advertisements.

14. The Administration advised that the Police set up the Cybercrime Policing Advisory Panel in December 2022, which sought to look into risks of crime and fraud involving AI (including deepfake technology) and to enhance public awareness on the potential risks of AI. The Administration would continue its efforts to enhance the anti-fraud awareness among the public through various channels. At the same time, the Police would step up online patrols and enforcement actions, and join forces with the Mainland and overseas law enforcement agencies in combating cross-boundary fraudulent activities.

Nurturing information security talent

15. Pointing out 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 better coordinating the work of upgrading the information security systems among various B/Ds and public organizations. The Administration replied that DPO and the Hong Kong Institute of Information Technology under the Vocational Training

Council signed a Memorandum of Understanding in January 2025 to jointly promote IT professional training in government departments and public organizations, including co-organizing a "Cybersecurity Certificate for the Public Sector" training programme. Continuous efforts would be made to enhance the cultivation of information security talent. Cybersecurity experts and organizations from the Mainland and overseas would be brought in to support the relevant work in Hong Kong.

Relevant papers

16. A list of the relevant papers available on the LegCo website is in the **Appendix**.

Council Business Divisions
Legislative Council Secretariat
6 October 2025

Appendix

Safeguarding information security

List of relevant papers

Committee	Date of meeting	Paper
Panel on Information Technology and Broadcasting	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
	14 October 2024	Agenda Item III: Work related to safeguarding and promoting information security Minutes of meeting
Finance Committee special meetings to examine the Estimates of Expenditure 2025-2026	11 April 2025	Administration's written replies to initial questions raised by Members on the Estimates of Expenditure 2025-2026 (Reply Serial No.: SB192) Minutes of meeting
Bills Committee on Protection of Critical Infrastructures (Computer Systems) Bill	13 March 2025*	Report of the Bills Committee

* Date of issue

Council meeting	Members' motion
29 November 2023	Members' motion: Combating cyber fraud crimes on all fronts Progress report

Council meeting	Members' motion
9 July 2025	Members' motion: Studying the enactment of a cyber security law and building a comprehensive system against cyber fraud Progress report

Council meeting	Question
5 July 2023	Question 6: Building a strong digital security barrier Question 13: Deception cases on social media platforms
18 October 2023	Question 17: Enhancing cyber security
15 November 2023	Question 9: Data governance system Question 14: Combating online and telephone frauds
22 November 2023	Question 11: Cybersecurity of government departments and other public organizations
17 January 2024	Question 3: Ensuring the normal operation of government electronic systems
29 May 2024	Question 6: Protection of personal data privacy Question 18: Cybersecurity of government departments and other public organizations
26 March 2025	Question 7: Information security of government departments and public organizations
7 May 2025	Question 7: Combating phishing