立法會
Legislative Council

LC Paper No. CB(2)1000/2026(04)

Ref: CB2/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 13 July 2026

Background brief on safeguarding information security

Purpose

This paper provides background information on the Administration's work in safeguarding information security. It also summarizes the major views and concerns raised by Members on relevant issues.

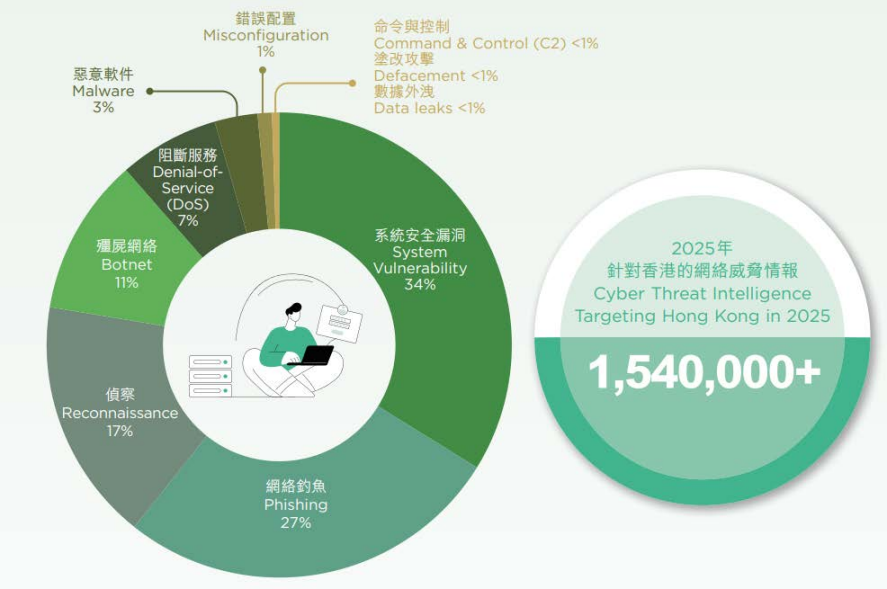
Background

2. To effectively address the evolving cybersecurity risks, the Administration has adopted a multi-pronged approach to enhancing information security in Hong Kong. The major measures include: (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 the community's overall cybersecurity awareness and defensive capability**; (c) **coordinating the handling of information security 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 security 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, **the Protection of Critical Infrastructures (Computer Systems) Ordinance** (Cap. 653) came into force on 1 January 2026. It aims to **safeguard the security of critical computer systems that maintain** the normal functioning of society by **imposing statutory obligations on critical infrastructure operators** ("CI operators"), thereby reducing the risk of essential services being disrupted or compromised by cyberattacks.

Overview of the local cybersecurity situation

4. According to information provided by the Hong Kong Police Force ("the Police"), over 1.54 million pieces of cyber threat intelligence specifically targeting Hong Kong were detected in 2025, primarily relating to system vulnerabilities (34%), phishing (27%) and reconnaissance activities (17%).



Source: Cybersecurity Report 2025

5. In addition, HKCERT handled a total of 15 877 **security incidents** in 2025, representing **an increase of approximately 27%** over 2024. These incidents mainly involved malicious activities such as phishing (56.5%), botnets (18%) and malware (9%). Meanwhile, the Police recorded a total of 31 571 **technology crimes** in the same year, representing **a 6.9% decrease** compared with 2024, with online deception cases accounting for 87.2% of the total. The figures for security incidents and technology crimes recorded in Hong Kong over the past three years are set out below:

	2023	2024	2025
Security incidents (including phishing, botnets and malware)	7 752	12 536	15 877
Technology crimes (including online deception, Internet blackmail and misuse of computer)	34 112	33 903	31 571

Sources: Website of HKCERT and papers submitted by the Administration to the Legislative Council on the law and order situation in Hong Kong (LC Paper Nos. CB(2)192/2025(01) and CB(2)174/2026(04))

Major views and concerns of Members

Preventing cyber fraud

6. Expressing concern about the growing prevalence of cyber fraud in Hong Kong in recent years, Members urged the Administration to **strengthen cooperation with overseas law enforcement agencies** to **combat transnational fraud syndicates and block fraudulent websites**, and **explore the enactment of a cybersecurity law** with a view to building a more comprehensive system against cyber fraud, thereby effectively tackling online disinformation and related fraudulent activities. Members also suggested that the Administration step up **anti-fraud publicity** through the mass media and channels such as "iAM Smart", while actively **tracing the sources of personal data leaks** and proactively monitoring the sale of personal data on the dark web, in order to prevent criminals from exploiting the leaked personal data for fraud or extortion.

7. The Administration advised that the existing legislation in Hong Kong could already effectively address certain aspects of cybersecurity. For example, the Crimes Ordinance (Cap. 200) would be invoked to prosecute offenders for the offence of "access to computer with dishonest intent", while "fraud" under section 16A and "obtaining property by deception" under section 17 of the Theft Ordinance (Cap. 210), among others, could be used for different kinds of fraudulent activities in various scenarios. The Administration had conducted intelligence exchanges and mounted joint law enforcement operations with a number of jurisdictions, as well as cooperating with international organizations such as the International Criminal Police Organization to combat cross-boundary cybercrimes. Furthermore, the Administration would closely monitor the progress of the Law Reform Commission's study on cybercrime and its final recommendations, and review the legislation in due course.

8. In terms of public education, apart from continuing to step up the promotion of cybersecurity and issuing anti-fraud alerts through diversified channels, the Administration would also conduct round-the-clock monitoring of online information (including the dark web) and take appropriate actions. At the same time, they would help local small and medium enterprises ("SMEs"), non-governmental organizations, and primary and secondary schools to address cybersecurity risks through various programmes and support measures, thereby fostering a secure and reliable cyber environment.

9. Members urged the Administration to **step up efforts in preventing and combating crimes involving the use of** emerging 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 fraudulent web pages or advertisements. Members also suggested **enacting dedicated legislation targeting AI-generated content** and **strengthening the regulation of online platforms** by, for example, requiring clear labelling of all AI-generated content.

10. The Administration advised that the Smart Policing Advisory Panel set up by the Police would look into the risks of crime and fraud involving AI (including deepfake technology) and raise public awareness of the potential risks of AI. At the same time, the Administration would continue its efforts to enhance the anti-fraud awareness among the public through various channels, and step up online patrols and enforcement actions, including collaborating with the Mainland and overseas law enforcement agencies in combating cross-boundary fraudulent activities. Furthermore, the Department of Justice had established an interdepartmental working group to review whether the laws under different policy areas could keep pace with technological developments (including AI), study ways to address the potential risks and regulatory requirements that might arise from the development and application of AI, identify loopholes and deficiencies in existing laws, and propose targeted and practical regulatory solutions by taking into account Hong Kong's actual circumstances.

<u>Enhancing information system security of government departments and public organizations</u>

11. In recognition of the Administration's work and effectiveness in coordinating the **cybersecurity attack and defence drill**, Members urged the Administration to **ensure that the daily operations** of the participating government departments and public organizations ("participating

organizations") **would not be affected**. Some Members suggested that the Administration should compare the drill results with the self-assessments of the participating organizations and put in place an incentive and penalty mechanism to encourage continuous improvement by the participating organizations.

12. The Administration advised that the cybersecurity attack and defence drill was conducted on a dedicated platform, enabling the attacker and defensive teams to carry out the drill under strict control. The attacker teams would only record the vulnerabilities identified during the simulated cyberattacks, and referees would assess whether intrusions were successful. The entire process would not affect the normal operation of relevant systems of the participating organizations. Upon completion of the drill, the participating organizations would be provided with reports on the results of the drill for follow-up action, so that they could strengthen their capabilities in identifying and responding to cyber incidents.

13. In response to Members' concern about the arrangements for **health checks on the information systems** of government departments, the Administration advised that since December 2024, the Digital Policy Office had been performing regular information security spot checks on all public-facing information systems of government departments, with a view to enhancing the identification of potential security vulnerabilities in the systems of various B/Ds, thereby preventing information security and cybersecurity incidents.

Information security of computing infrastructure

14. In view of the commissioning of the Cyberport's Artificial Intelligence Supercomputing Centre ("AISC") and the future development plans for the Sandy Ridge Data Facility Cluster, Members expressed concern about how the Administration would make forward-looking arrangements to **build a robust cyber and data security shield for computing infrastructure** in Hong Kong. The Administration advised that $100 million had been set aside to strengthen AISC's cyber and data security, including data protection, security monitoring, audit and risk assessment services, and to provide training and educational activities on cyber and data security for users of the AISC services.

Helping small and medium enterprises respond to cybersecurity risks

15. Expressing concerns about the Administration's measures in place to **help SMEs respond to cybersecurity risks**, Members suggested that the Administration should collaborate with sizeable organizations or trade associations to provide support for 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 and setting up staff training platforms, thereby enhancing the awareness and capabilities of the industry and the general public in safeguarding cybersecurity. The Administration would also collaborate with HKIRC to promote publicity, education and training on cybersecurity, and provide the "Healthy Web" service and information security incident response support. In addition, the Administration were studying enhancements to the "Digital Transformation Support Pilot Programme", which would provide subsidies on a matching basis to encourage SMEs to adopt readily available basic digital technology solutions, such as AI and cybersecurity, thereby enhancing their competitiveness and information security.

Supply of cybersecurity talents

16. Members considered that the Administration should take various measures to **attract** more **cybersecurity talents to pursue development in Hong Kong**, while providing training for relevant staff within the Government and designated CI operators under the Protection of Critical Infrastructures (Computer Systems) Ordinance, so as to ensure that the government departments and CI operators would comply with the relevant statutory and administrative requirements.

17. The Administration pointed out that it would proactively attract overseas cybersecurity talents through various talent admission schemes (e.g. by including "experienced cybersecurity specialists" and "information technology technicians" under the Talent List and the Technical Professional List respectively), thereby assisting the industry in attracting cybersecurity talents from the Mainland and overseas. The Administration were also committed to building a cybersecurity ecosystem to attract relevant enterprises to establish a presence in Hong Kong and bring in more talents. Furthermore, thematic seminars and staged training courses would be provided for senior management and technical staff of the Government, and assistance would be given to CI operators for launching promotion, training and regular drills related to the Protection of Critical Infrastructures (Computer Systems) Ordinance, with a view to enhancing staff awareness and preparedness regarding cybersecurity.

Relevant papers

18. A list of relevant papers on the Legislative Council website is in the **Appendix**.

Council Business Divisions
Legislative Council Secretariat
6 July 2026

Appendix

Safeguarding information security

List of relevant papers

Committee	Date of meeting	Paper
Panel on Information Technology and Broadcasting	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
	13 October 2025	Agenda Item II: Work on safeguarding information security 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	Paper
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

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