LC Paper No. CB(2)1860/2025(01)

For discussion
on 13 October 2025

Legislative Council
Panel on Information Technology and Broadcasting

Work Related to Safeguarding Information Security

PURPOSE

This paper briefs Members on the latest situation of information security in Hong Kong and the Government's work related to safeguarding information security.

OVERALL SITUATION OF INFORMATION AND CYBER SECURITY

2. Established and operated by the Hong Kong Productivity Council (HKPC), the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) handled a total of 15 722 information security incidents in the past year (September 2024 – August 2025). Among them, the main categories of information security incidents were phishing (8 973 cases), botnets (3 337 cases) and malware (1 403 cases). As compared with the same period last year, the number of malware cases increased at a relatively high rate. A breakdown of statistics on these information security incidents is at **Annex I**.

3. Regarding government information security incidents, under the current response mechanism, all government departments are required to report any information security incident to the Digital Policy Office (DPO). In the first eight months of 2025, the DPO received a total of eight reports of information security incidents, with a decrease from 14 in the same period last year. These incidents involved defacement of websites and loss of mobile devices or removable media containing confidential information.

4. In addition, the Hong Kong Police Force (HKPF) recorded a total of 33 903 technology crime cases in 2024, representing a slight decrease from 2023, with a cumulative amount of losses reaching HK$5.13 billion,

representing a decrease of 6.7% from 2023. Among them, there were 61 cases of "hacking activities", with a relatively significant increase in both the number of cases and amount of losses. In the first seven months of 2025, a total of 19 080 technology crime cases were recorded, representing a slight decrease over the same period last year, while the cumulative amount of losses increased to about HK$3.64 billion. A breakdown of statistics on the technology crimes is at **Annex II**.

5. In the case of personal data, the Office of the Privacy Commissioner for Personal Data (PCPD) received a total of 151 personal data breach incident notifications in the first eight months of 2025, representing an increase of nearly 10% from 140 cases in the same period of 2024. Among them, there were 55 cases of personal data breach involving hacker intrusions, comparable to the number of cases in 2024.

SAFEGUARDING INFORMATION SECURITY IN THE GOVERNMENT

6. Information and cyber security are the cornerstone of digital government. The Government has all along been adopting a multi-pronged strategy to strengthen information and cyber security of all policy bureaux/departments (B/Ds), which include the introduction of various measures to enhance information system governance and security in August 2024 and the promulgation of the revised "IT Security Policy and Guidelines" in April 2025. Currently, all B/Ds have assigned senior directorate officers and Head or Deputy Head of public bodies under B/Ds' purview to be responsible for information security work and project management of their essential information systems, ensuring compliance of B/Ds and public bodies with the relevant information security requirements. The implementation of related measures are as follows:

(I) Enhancing information system security and stability

- Additional stress and cyber security tests: all B/Ds and public bodies under their purview have arranged additional stress tests and cyber security tests by an independent third party before rollout of information systems with major impact on the general public in accordance with the requirements. In addition, the DPO has requested B/Ds to subject large-scale and high-risk information systems to additional stress tests and cyber security tests to be conducted by an independent third party arranged by the DPO prior to system launch, with a view to assisting B/Ds in assessing the system's response to abnormal or extreme loading, and enhancing their resilience capabilities in responding to cyber attacks. As at August 2025, the DPO, B/Ds and public bodies under their purview have arranged the additional tests for more than 80 specified projects.

- Regular monitoring and self-assessment: as required by the DPO, all B/Ds and public bodies under their purview have established a standing monitoring mechanism on their information system, and conducted self-assessments such as security risk assessment and audit, privacy impact assessment, regular system checking and penetration tests during the business-as-usual stage. The DPO has provided appropriate technical advice, guidelines and best practice guides to B/Ds.

- System health check: the DPO has introduced a centralised cyber security health check platform since December 2024 to conduct regular and continuous health checks on government public-facing information systems and websites to enhance the ability to identify potential security vulnerabilities in B/Ds' systems, thereby bolstering the prevention of information and cyber security incidents.

- Compliance audit: the DPO launched a new round of government-wide information security compliance audit in September 2024 and has completed the audits for all B/Ds by August 2025. In addition, starting from 2025, the DPO will identify no less than eight important government information technology (IT) systems every year under a risk-based approach for in-depth information security compliance audit, so as to ensure B/Ds' compliance with government information security regulations. The technical review and assessment of five out of the nine selected systems this year have been substantially completed, while the remaining system audits are underway and expected to be completed by year-end.

- Cybersecurity attack and defence drill: the DPO has co-ordinated and organised annual cybersecurity attack and defence drill since 2024. The second cybersecurity attack and defence drill was launched in October 2025. Based on the successful experience of the first drill last year, the scale of this year's drill has been expanded to include the participation of 25 government departments and nine public organisations forming the defensive teams, and 14 attacker teams formed by cyber security enterprises and post-secondary colleges, thereby enhancing the drill effectiveness. Experienced teams from the Mainland were also invited to participate in the attacker teams this year to promote technical exchanges between the two places.

(II) Strengthening staff training and support

- Staff training: the DPO and the Civil Service College closely collaborate to organise regularly thematic seminars under the Innovation and Technology leadership series to strengthen the core skills of senior management of all B/Ds in using digital technology, covering topics such as project governance, cyber security and artificial intelligence (AI). Since the first thematic seminar held in November 2024, about 260 senior directorates from various B/Ds have attended such seminars. Moreover, in 2024-25, the DPO arranged more than 100 training courses related to core digital skills for government staff, covering more than 9 700 participants. The DPO will continue to organise different types of training for government staff with the aim of enhancing their awareness of and readiness for information and cyber security.

- Refresher courses: the DPO commissioned the Hong Kong Institute of Information Technology (HKIIT) under the Vocational Training Council (VTC) to design and organise the "Certificate in Cybersecurity for the Public Sector" course, aiming to comprehensively enhance the information security skills of government staff. The course covers three levels: "Foundation", "Intermediate" and "Advanced". As at August 2025, 584 and 173 government staff have completed the "Foundation" and "Intermediate" courses respectively.

- Anti-phishing drills: the DPO launches the new round of "Government-wide Phishing Drill Campaign" in 2025, which makes use of new technologies such as AI to simulate phishing emails, thereby heightening government staff's awareness and ability to identify such frauds.

(III) Strengthening collaboration with the industry

- Collaboration with cyber security industry: in response to recent frequent cyber security threats, the DPO, together with the

Internet Infrastructure Liaison Group [1] and cyber security industry, held a meeting in July 2025 to discuss enhancement of technical protective measures and risk management strategies. In view of a number of major events in the second half of the year, including the 15th National Games and the eighth-term Legislative Council (LegCo) general election, the DPO will enhance real-time threat monitoring and intelligence sharing as well as conduct attack and defence drills to ensure the robust operation and thorough deployment of relevant critical information systems.

PROMOTING INFORMATION SECURITY AT SOCIETY LEVEL

7. A secure and reliable Internet environment is a prerequisite for the development of digital economy and smart city. The Government is committed to close collaboration with stakeholders such as the Hong Kong Internet Registration Corporation Limited (HKIRC) and HKCERT to implement various plans and support measures, with a view to raising the public awareness of information security and supporting the industry in addressing cyber security risks. The related measures are as follows:

(I) Enhancing enterprises' capability in responding to cyberattacks

- Free website checking services and cyber security vulnerability testing: supported by the DPO, the HKIRC launched a free and integrated security service named "Cybersec One" in March 2025, helping small and medium enterprises (SMEs), non-profit organisations and schools to identify website vulnerabilities, conduct risk assessments and provide solutions such as recommending free resources, to empower them to strengthen their cyber security resilience.

  At the same time, the HKIRC continues to implement the free website security checking service "Healthy Web" to proactively alert ".hk" users the potential cyber risks and provide free in-depth website security scanning services and telephone consultation for them to take early precautions. As at August 2025, the HKIRC has provided about 52 000 times of checking service to ".hk" users.

[1] The group is chaired by the Deputy Commissioner (Digital Infrastructure) of the DPO, with members comprising representatives from the DPO, HKCERT, Hong Kong Internet Exchange (HKIX), HKIRC, Hong Kong Internet Service Providers Association (HKISPA), Hong Kong Police Force (HKPF) and the Office of the Communications Authority (OFCA).

Besides, the HKPF, the PCPD and the cyber security industry co-organised the third annual "Bug Hunting Campaign" from June to August 2025, adopting AI technology to provide free cyber security vulnerability testing to SMEs with limited resources and conduct security audits on their AI applications. The participating enterprises will receive detailed cyber security reports and one-on-one professional consultation services, so that they can take appropriate measures to enhance their overall security protection level.

The 2025 Policy Address also announced the enhancement of Cyberport's Digital Transformation Support Pilot Programme to provide SMEs with subsidies, on a matching basis, to empower enterprises to apply AI and cyber security solutions for enhanced competitiveness and information security.

- Cyber security information sharing: to strengthen connection between cyber security service providers and local enterprises and organisations, the DPO partnered with HKCERT to launch the "Cybersecurity Service Providers Connect Programme" in July this year. A dedicated platform will be launched to showcase categorised and vetted cyber security solutions, helping service providers approach more potential clients while enabling businesses to find trusted cyber security solutions.

- Free online staff training: to raise the cyber security awareness and knowledge of enterprises across various industries and their staff, the HKIRC launched the "Cybersec Training Hub", which provided free online cyber security training to staff across various industries. As at August this year, more than 372 000 attendees have enhanced their knowledge and skills through the platform.

- Cybersecurity Recognition Scheme: to encourage enterprises to actively raise their employees' cyber security awareness, HKIRC and ISACA China Hong Kong Chapter co-organise the annual "Cyber Security Staff Awareness Recognition Scheme" to recognise organisations that have successfully enhanced staff awareness of cyber security within their organisations over the past year. In 2024-25, the scheme has attracted over 80 SMEs and large enterprises from banking, property management, retail and other industries to participate.

(II) Stepping up public education

- Promoting cyber security: to raise the cyber security awareness of the community, the DPO supports the “China Cybersecurity Week” and collaborates with industry players to organise a variety of promotional activities every year. With a theme of “Let’s Secure as we Digitalise” this year, the DPO organised a series of activities such as Hong Kong forum, Cyber Security Technology Summit Hong Kong, Instant Messaging Apps Stickers Design Contest and publicity activities. In addition, the DPO continues to enhance and update the “InfoSec” and “Cyber Security Information Portal” thematic websites from time to time, including adding educational videos and latest information to brief the general public about the prevailing trends of cyber security, as well as the practical skills to prevent cyberattacks effectively.

- Protection of personal data: the PCPD proactively promotes measures to the general public to strengthen personal data protection. The PCPD not only raises the public’s awareness on personal data protection through different promotional channels, but also proactively communicates and collaborates with the industry through publishing guidance notes, pamphlets and booklets related to personal data security, including a series of publications related to AI (for example, Checklist on Guidelines for the Use of Generative AI by Employees, model framework and leaflet on Personal Data Protection related to AI, leaflet providing tips on the safe use of AI chatbots), Guidance on Cloud Computing, leaflets on smart use of smartphones and social media, Guidance Note on Data Security Measures for Information and Communications Technology, etc, so as to assist the industry to comply with the relevant requirements under the Personal Data (Privacy) Ordinance.

- Fortify defences against deception: the HKPF has been adopting a multi-channel strategy to promote public awareness against fraud. Targeting online shopping fraud, especially the rising trend of fraud cases related to the concert tickets, the HKPF has issued alerts via various channels such as their “CyberDefender” website, Facebook page and television programmes, and organised a large-scale press conference to expose online ticket fraud methods and provide preventive measures. For the first time, the HKPF also took the initiative to contact the concert organisers to co-ordinate the issuance of antiscam alerts through official channel, and called on the public to use the "Scameter" to verify the credibility of sellers before the transactions.

In addition, the HKPF launched "Scameter" and relevant mobile application, issuing more than 1 200 000 alerts on frauds and cyber security risks as of 1 September, 2025. The "Scameter+" has also been upgraded to include alerts and a public reporting platform. Furthermore, the "Suspicious Account Alert" has been launched to remind the public to stay alert of scams. The mechanism has been expanded to cover Faster Payment System, online banking, over-the-counter transfers and transactions by Automatic Teller Machines since December 2024 to better protect the public.

(III) Promoting cross-territory co-operation

- Regular contacts and exchanges: the Government Computer Emergency Response Team Hong Kong actively participates in international co-operation fora and maintains close contact with other regional computer emergency response teams (CERT) through joining the international CERT Coordination Centre, the Forum of Incident Response and Security Teams and the Asia Pacific Computer Emergency Response Team (APCERT), as well as regularly participates in technical exchanges such as APCERT incident response drills.

- Symposiums: the Government has participated in the annual "World Internet Conference Wuzhen Summit" organised by the Cyberspace Administration of China, and delivered keynote speeches at various forums to share the latest developments of innovation and technology (I&T) and cyber security in Hong Kong. In April 2025, the "World Internet Conference Asia-Pacific Summit" organised by the World Internet Conference, hosted by the HKSAR Government and co-organised by the Innovation, Technology and Industry Bureau, was held in Hong Kong for the first time. In addition to a dialogue session and a forum, a series of affiliated activities including a cyber security emergency response advanced training programme were also held.

  In December last year, the DPO collaborated with the HKIRC to organise the "Cybersecurity Symposium 2024", which brought together top-notch cyber security experts from Hong Kong and the Mainland to jointly explore how to strengthen Hong Kong’s overall defence and resilience capabilities against cyberattacks with a total attendance of nearly 1 000. In May this year, the DPO and the HKPF co-organised the “Cybersecurity & Diverse Innovation Symposium 2025” with an attendance of over 600 local and Mainland experts from different sectors to explore the latest cyber security challenges, cross-sector collaboration, and innovation-driven defence strategies.

- Memorandum of Understanding: in September 2024, the DPO signed the “Memorandum of Understanding (MoU) on Facilitating Cybersecurity Exchange and Collaboration in Guangdong-Hong Kong-Macao” with the Cyberspace Administration of Guangdong Province and the Comissão para a Cibersegurança of Macao SAR. The MoU strengthens co- operation in the aspects of technological exchange, information sharing and emergency response measures among Hong Kong, Guangdong Province and Macao SAR. In May this year, the DPO attended the Guangdong/Hong Kong/Macao Cybersecurity Joint Conference held in Shenzhen to promote the areas of collaboration in the MoU, share the latest status of cyber security work, and discuss the focus of cyber security co- operation among Guangdong, Hong Kong and Macao in 2025.

(IV) Making legislation and guidelines

- Computer-system security of critical infrastructures: the LegCo passed the Protection of Critical Infrastructures (Computer Systems) Ordinance on 19 March 2025. The Ordinance imposes statutory obligations on designated operators of critical infrastructures to ensure that they adopt appropriate measures to protect their computer systems and minimise the risk of essential services being disrupted or compromised due to cyberattacks, thereby enhancing the overall cyber security in Hong Kong. The Ordinance will come into effect on 1 January 2026. The Commissioner’s Office under the Security Bureau will be set up on the same day to enforce the Ordinance.

- Data centre infrastructure security: having regard to the latest national and international data centre security management standards and practices, the Government’s internal guidelines, as well as experience gained from the construction and operation of the Government Data Centre Complex, the DPO published the

"Practical Guide on Data Centre Security" in December 2024 as an industry reference on security management, design principles, technology, operation and maintenance of data centres, in order to enhance the security of Hong Kong's data centre infrastructure.

HUMAN RESOURCES DEVELOPMENT

(I) Cultivating local talents

Primary and secondary schools

8. The Government attaches great importance to nurturing digital literacy and skills among students through basic education. The Education Bureau (EDB) has developed the "Information Literacy for Hong Kong Students" Learning Framework to support schools in cultivating students' capability and attitude to use information and communication technology efficiently and ethically in their learning and daily life, including teaching students about the importance of information and cyber security and personal data privacy protection. In collaboration with relevant organisations including the Hong Kong Journalism Education Foundation and the HKPF, the EDB has also launched learning and teaching resources on media and information literacy and a series of videos. Teacher professional development programmes have also been organised to support teachers in strengthening media and information literacy of students both inside and outside the classroom. At the same time, in conjunction with the promotion of digital education (including AI education) in primary and secondary schools, the EDB will establish an "AI Literacy" learning framework to further enhance students' information literacy.

9. Beyond the regular curriculum, the DPO implements the "IT Innovation Lab in Secondary Schools" and the "Knowing More About IT" programmes which subsidise secondary and primary schools respectively to launch extra-curricular activities (ECAs) related to IT, including cyber security-related competitions, workshops, courses, etc. As at August this year, over 1 000 schools have organised about 7 300 activities under the two programmes, which included cyber security-related ECAs such as introductory courses and technical workshops on cyber security. In addition, the DPO has launched a school visit programme to disseminate cyber security messages to students, teachers and parents. In the 2024/25 school year (as at June this year), the DPO held cyber security talks for

over 5 100 teachers and students in 21 schools to enhance their understanding of cyber security.

Post-secondary programmes

10. At the post-secondary education level, institutions have been proactively stepping up I&T education in recent years, including offering more information and cyber security-related programmes with increased student intake. To meet Hong Kong’s social and economic needs, the “Study Subsidy Scheme for Designated Professions/Sectors” (SSSDP) launched by the EDB provides subsidies to encourage the self-financing post-secondary education sector to offer programmes in ten disciplines such as computer science (covering cyber security). In the 2025/26 academic year, the SSSDP covers six undergraduate and two sub-degree programmes in the computer science discipline, involving a total of 435 subsidised places, which represents a nearly 10% increase compared with the 2024/25 academic year.

11. Furthermore, with the support of the Government, the VTC established the HKIIT in November 2023, which focuses on providing IT and other related technology programmes to consolidate the IT capabilities of Hong Kong and respond to the manpower demand of the industry. In the 2024/25 academic year, the HKIIT admitted its first cohort of students and offered a total of 21 programmes, comprising 11 full-time Higher Diploma (HD) programmes, 2 full-time Diploma in Foundation Studies (DFS) programmes, and 8 part-time HD programmes. These programmes cover areas such as cyber security, AI, and cloud and data centre administration. A total of 2 111 new students were admitted to 13 of its full-time HD and DFS programmes. The HKIIT will continue to expand and update its curricula based on market needs and technological development trends with a view to nurturing a comprehensive pool of IT professionals.

Retraining, continuing education and in-service training

12. On local workforce training, the Employees Retraining Board currently offers eligible employed persons with over 700 regular training courses straddling across 28 industries and generic skills, including courses in the cyber security and management field. Hong Kong residents aged 18 or above may also make use of the Continuing Education Fund to enrol in courses relating to computer science and IT.

13. To realise the Government’s mission to enlarge the local talent pool in information security and to promote talent exchange and

co-operation between Hong Kong and the Mainland in the field of information security, the China Information Technology Security Evaluation Center authorised the Hong Kong College of Technology in late 2024 and collaborated with the HKIIT under the VTC to provide Certified Information Security Professional (CISP) training programmes. This enables professionals in Hong Kong to obtain the nationally recognised cyber security professional qualification locally, enhancing the professional skills and competitiveness of local information security practitioners.

14. The DPO, the HKIRC and the HKPF jointly organised the "Cyber Attack and Defence Elite Training cum Tournament" again in July 2025, which gained extensive support and active participation from academia and industry. Through a series of free training and competitions, the event provided elites from academia and industry with a platform to practise and exchange knowledge, and enhanced their incident response capabilities through simulated combats, with a view to nurturing a new generation of cyber attack and defence experts.

15. Moreover, the DPO, the HKPC and the HKCERT jointly organised "HKCERT Capture the Flag Challenge" in January 2025, which also featured an international category. In addition to effectively enhancing the cyber attack and defence capabilities of participants and nurturing local cyber security professionals, the event provided an internationalised exchange platform that facilitated exchange among global cyber security talents.

(II) Attracting Mainland and overseas talents

16. The Government actively attracts cyber security talents from the Mainland and overseas to enlarge the local cyber security talent pool. The "Technology Talent Admission Scheme" (TechTAS) provides a fast-track arrangement for eligible companies to admit Mainland and overseas technology talents to undertake research and development work for them. As at end-August this year, a total of 40 non-local persons from the cyber security sector were approved for entry under TechTAS. The Government has also included in the "Talent List" a number of professions in the I&T segment, such as "experienced cyber security specialists", to facilitate the admission of technology talents by industry through relevant admission schemes. According to the Immigration Department, as of end-August this year, a total of 48 applications that had met the criteria of "experienced cyber security specialists" on the "Talent List" have been approved under the "Quality Migrant Admission Scheme", the "General

Employment Policy” (GEP) and the “Admission Scheme for Mainland Talents and Professionals” (ASMTP).

17. In addition, the Government introduced the Technical Professional List in end-May 2025, which includes “IT technicians” among the eight specified skilled trades. Mid-level non-degree technical professionals who are engaged in the three scopes of work of cyber security, network support and program development, and aged between 18 and 40, may be allowed to settle and advance their careers in Hong Kong through the new channels offered under the GEP and the ASMTP, enriching talent resources for local industry. This new arrangement will be piloted for three years with an overall quota of 10 000, and the quota for each skilled trade is limited to 3 000. The Technical Professional Stream has started accepting online applications since 30 June this year.

ADVICE SOUGHT

18. Members are invited to note the content of this paper and offer comment.

Innovation, Technology and Industry Bureau
Digital Policy Office
October 2025

Annex I

Breakdown of Statistics on Information Security Incidents Handled by The Hong Kong Computer Emergency Response Team Coordination Centre

Incident Category	September 2023 to August 2024		September 2024 to August 2025	
	Number of Cases	**%**	**Number of Cases**	**%**
Phishing (phishing websites)	6 141	58	8 973	57
Botnet (zombie computer)	2 663	25	3 337	21
Malicious Software (including ransomware)	618	6	1 403	9
Hacker Intrusion/ Web Defacement	19	<1	11	<1
Distributed Denial-of-Service (DDoS) Attacks	2	<1	4	<1
Others [2]	1 140	11	1 994	13
Total:	**10 583**	**100**	**15 722**	**100**

[2] Including identity theft, data leakage, etc.

Annex II

Statistics on Technology Crime Cases Handled by The Hong Kong Police Force and the Resultant Monetary Loss

	2024	**2025 (as of July)**
Case Nature	**Number of Cases**	**Number of Cases**
Internet Deception	**27 485**	**16 748**
（i） *Online Business Fraud*	*12 215*	*7 924*
- *E-Shopping Fraud*	*11 559*	*7 594*
- *Credit Card Misuse*	*656*	*330*
（ii） *Email Scam*	*197*	*69*
（iii） *E-Banking Fraud*	*20*	*19*
（iv） *Social Media Deception*	*3 039*	*1 347*
（v） *Miscellaneous Fraud* *(including online investment fraud)*	*9 283*	*6 631*
（vi） *Phishing Scam*	*2 731*	*758*
Internet Blackmail	**2 559**	**915**
（i） *Naked Chat*	*2 434*	*857*
（ii） *Other Internet Blackmail*	*125*	*58*
Misuse of Computer	**3 055**	**960**
（i） *Unauthorised Access To Online Service Accounts*	*2 989*	*935*
（ii） *Hacking Activities*	*61*	*24*
（iii） *DDoS Attack*	*5*	*1*
Others	**804**	**457**
Total (number of cases):	**33 903**	**19 080**
Monetary Loss (in $ million)	**5,129.0**	**3,639.4**