For discussion
on 13 July 2026

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. As the application of artificial intelligence (AI) technology becomes increasingly widespread, it also poses new challenges to the information security. Over the past year, AI-driven cyberattacks have attracted significant attention as they threaten information protection and overall network security. In this connection, the Government, enterprises and citizens should raise cyber security awareness, thereby enhancing the overall information and cyber security defence capabilities of society continuously.

3. The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) under the Hong Kong Productivity Council handled a total of 15 740 information security incidents from June 2025 to May 2026, representing an increase of 5% compared with the same period last year. Of these, 9 764 cases involved phishing, up by 14.2%, while the number of incidents related to botnets (2 396 cases) and malware (1 288 cases) decreased by 32.7% and 6.1% respectively compared with the same period last year. A breakdown of statistics on relevant information security incidents is at **Annex I**.

4. In addition, the Hong Kong Police Force (HKPF) recorded a total of 11 565 technology crime cases from January to May 2026, representing a decrease of 13.9% from the same period in 2025, with a cumulative

amount of losses reaching HK$2.07 billion, dropping by 17.1% from the same period in 2025. While most types of crime had recorded a reduction, theft of online accounts and phishing saw relatively significant increases. There were no deepfake-related scams recorded during the period. A breakdown of statistics on relevant technology crimes is at **Annex II**.

5. In the case of personal data security, the Office of the Privacy Commissioner for Personal Data (PCPD) received a total of 148 personal data breach incident notifications in the first six months of 2026, representing an increase of 53% from 97 cases in the same period of 2025. Among them, there were 58 cases of personal data breach involving hacker intrusions, representing an increase of 66% from 35 cases in the same period of 2025.

6. Regarding government information security incidents, in the first five months of 2026, the Digital Policy Office (DPO) received two reports of information security incident from government departments that involved compromise of protected information systems or data assets, and loss of mobile devices or removable media containing confidential information, seeing a drop from five reports in the same period of 2025.

BUILDING CYBER SECURITY DEFENCE CAPABILITIES OF SOCIETY

7. The Government continues to collaborate closely with stakeholders such as the HKCERT and the Hong Kong Internet Registration Corporation Limited (HKIRC) to implement various programmes and support measures, with a view to enhancing public awareness and vigilance regarding information security and AI, and supporting the industry in defending against cyber security risks. The related measures are as follows:

(I) Enhancing capability of local enterprises in responding to cyberattacks

- **Free website checking services and cyber security vulnerability testing**: The HKIRC, together with the DPO and the Cyber Security and Technology Crime Bureau of the HKPF, expanded the integrated security service named "CyberSec One" to **"Cybersec One+"** in June this year. The scope of the beneficiaries extended from the existing local small and medium enterprises (SMEs), non-governmental organisations (NGOs) and

primary and secondary schools to the general users, providing website security testing, risk assessment and professional improvement recommendations for different types of stakeholders.

- **<u>Cyber security information sharing</u>**: The DPO partnered with the HKCERT to launch the **"Cybersecurity Service Providers Connect Programme"** in July last year, providing a dedicated platform for eligible cyber security service providers and local enterprises and organisations to connect. As at May this year, 25 service providers have successfully passed the assessment. The platform is currently being enhanced with new features expected to roll out in October this year, with a view to helping local organisations find suitable cyber security solutions more effectively and conveniently.

- **<u>Free online staff training</u>**: The HKIRC has been offering the **"Cybersec Training Hub"** since August 2022, providing free online cyber security training to staff across various industries. As at May this year, more than 484 000 attendees have enhanced their knowledge and skills through the platform.

- **<u>Cybersecurity Recognition Scheme</u>**: The HKIRC and the Information Systems Audit and Control Association China Hong Kong Chapter co-organise the annual **"Cybersecurity Staff Awareness Recognition Scheme"** to encourage and recognise organisations that have actively enhanced staff awareness of cyber security over the past year. In 2025-26, the scheme attracted participation from about 100 SMEs and large enterprises.

(II) Deepening public awareness

- **<u>Promoting safe AI applications</u>**: In response to the latest development, the DPO has launched a series of AI-related cyber security initiatives. These include co-organising with the HKIRC the **"Secure AI@Work Enablement Campaign 2026"** in June this year to advocate the safe application of AI technologies in the workplace by SMEs, NGOs and public organisations. By providing practical resources that promote good cyber security practices, the campaign aims to foster a sustainable culture of AI and cyber security awareness across the community.

Concurrently, the DPO together with the Hong Kong Cybersecurity Professional Association, etc will co-organise the **"AI x Cybersecurity Challenge"** for the first time from July to August this year. Participating teams shall design, build and operate AI-driven systems that automatically analyse the cyber range provided by the organisers, and identify and exploit vulnerabilities, thereby driving the efficiency of AI-powered cyber defence and demonstrating the potential of "AI versus AI".

The DPO, the HKIRC and the HKPF will jointly organise the **"Cyber Attack and Defence Elite Training cum Tournament"** again in August this year. It will incorporate AI technologies and offer free professional training and simulated practical exercises to enhance participants' offensive-defensive capabilities and AI collaboration literacy, enabling them to effectively leverage AI technologies to counter cyber threats and nurture cyber security professional talent.

The HKPF and Cyberport jointly established the **"Smart Policing Joint AI Lab"** in May this year, launching two AI research and development projects on anti-deepfake technology and cyber defence technology. By building strategic public-private partnerships, the initiative creates an open, flexible and forward-looking collaborative platform to address the increasingly complex challenges of digital policing.

- **<u>Fortifying defences against deception</u>**: In the face of a constant stream of technology crimes, the HKPF is actively adopting a multi-channel promotional strategy to broaden the reach of cyber security education. In response to the surge in online investment scams, online shopping fraud and phishing attacks in recent years, the HKPF disseminates anti-fraud alerts widely through the **"CyberDefender"** website, Facebook page and television programmes, as well as rolls out another upgrade to the **"Scameter"** app in October last year by integrating an AI analytics engine, thereby greatly enhancing its intelligence processing capability to improve overall anti-fraud effectiveness.

  Through the "Cyberdefenders Alliance" platform, the HKPF, together with the Education Bureau (EDB) and the DPO, launched the "CyberDefenders' Alliance Card Game" in October last year, alongside the anti-fraud teaching kits, to promote across primary and secondary schools throughout Hong Kong, helping young people improve digital literacy and fraud awareness through play.

The HKPF also held the first "Cyberdefenders Alliance" inter-school championship from December last year to March this year, attracting over 15 000 students from more than 100 primary and secondary schools.

- **Promoting cyber security**: To support the annual "China Cybersecurity Week", the DPO will collaborate with industry players to organise a variety of activities under this year's theme "Innovate with Grace, Peace in Cyberspace", including China Cybersecurity Week Hong Kong Sub-forum, AI-Generated Four-Panel Comic Contest, tram advertising campaigns, etc.

(III) Making legislation and guidelines

- **Computer-system security of critical infrastructures**: To enhance protection of computer systems that support critical infrastructure, the Protection of Critical Infrastructures (Computer Systems) Ordinance came into effect on 1 January this year, imposing statutory requirements on designated operators of critical infrastructures to ensure that they adopt appropriate measures to safeguard the computer-system security of critical infrastructures that maintain the normal functioning of society and minimise the chance of essential services being disrupted or compromised by cyberattacks, thereby enhancing the overall computer-system security in Hong Kong. The Office of the Commissioner of Critical Infrastructure (Computer-system Security) under the Security Bureau is responsible for enforcing the Ordinance and related duties, and has issued various Codes of Practice providing practical guidance to operators on fulfilling their responsibilities.

- **Reviewing and studying AI and data security legislation**: We will explore how to further strengthen Hong Kong's governance competence in addressing AI and data risks, application safety, governance standards and cyber security through statutory and regulatory governance frameworks, while fully supporting the "Inter-Departmental Working Group to Review Legislation to Support Wider Application of AI" established by the Department of Justice which will conduct a comprehensive and thorough review of existing laws, and then explore targeted and practicable solutions taking into account Hong Kong's actual circumstances.

- **<u>Personal data privacy</u>**: The PCPD has issued guidelines on data security protection and actively assists the industry in complying with the relevant requirements of the Personal Data (Privacy) Ordinance (PDPO). In light of the rising public concern over personal data breach incidents in recent years, the Government has been working closely with the PCPD in exploring enhancements to the PDPO with a view to effectively preventing personal data breach incidents.

(IV) Human Resources Development

- Post-secondary institutions have been proactively stepping up innovation and technology (I&T) education in recent years, including offering more information and cyber security-related programmes with increased student intake. 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 2026/27 academic year, the SSSDP covers six undergraduate and three sub-degree programmes in the computer science discipline, involving a total of 475 subsidised places, which represents a nearly 10% increase compared with the 2025/26 academic year.

  To further enhance the professional capabilities of local information security practitioners, the Hong Kong College of Technology and the Hong Kong Institute of Information Technology (HKIIT) continue to jointly provide Certified Information Security Professional training programmes, enabling professionals in Hong Kong to obtain the nationally recognised cyber security professional qualification locally. As at May this year, a total of 733 participants have completed the training programmes.

(V) Promoting cross-territory co-operation

- **<u>Regular contacts and exchanges</u>**: The Government Computer Emergency Response Team Hong Kong and the National Computer Network Emergency Response Technical Team/Coordination Center of China have set up a mechanism for reporting cyber threats and attacks to strengthen exchange and co-operation, enhance sharing of information security intelligence and foster collaborative response capabilities.

- **<u>Symposiums</u>**: The "World Internet Conference Asia-Pacific Summit" was held in Hong Kong again in April this year. In addition to dialogue sessions and forums, activities organised included a cyber security training programme and themed salon, etc. The Government also participates annually in the "World Internet Conference Wuzhen Summit" to attend various forums to share the latest developments of I&T and cyber security in Hong Kong. In January this year, the DPO collaborated with the HKIRC to organise the third "Cybersecurity Symposium", attracting nearly 1 000 cyber security experts and industry professionals. Also this year, the DPO will merge two flagship events, the "Cyber Security Summit Hong Kong" and the "Cybersecurity Symposium", into the larger-scale "Cyber Security Symposium and Summit".

- **<u>Memorandum of Understanding</u>**: The Innovation, Technology and Industry Bureau signed the Memorandum of Understanding on Co-operation in Innovation and Technology Development in April this year with the Cyberspace Administration of China to deepen the implementation of the National 15th Five-Year Plan and supporting Hong Kong's development into an international I&T centre. Both sides will further strengthen co-operation, jointly propel new quality productive forces development, deepen co-operation in cyber security and strengthen international exchanges and promotion.

SAFEGUARDING INFORMATION SECURITY IN THE GOVERNMENT

8. Information security and cyber security are anchor to drive the continuous development of digital government. The Government has all along been adopting a multi-pronged strategy to strengthen the information and cyber security of all policy bureaux/departments (B/Ds). Implementation of related measures is as follows:

(I) Enhancing information system security and stability

- **<u>Cybersecurity attack and defence drill</u>**: The second cybersecurity attack and defence drill co-ordinated by the DPO was held in October 2025 with an expanded scale. The third drill will take place in October this year. In addition to more

government departments and public organisations, private organisations will also be invited to participate in the drill.

- **Compliance audit**: Starting from last year, the DPO identifies no less than eight important government information systems every year under a risk-based approach for in-depth information security compliance audit, thereby assisting them in continuously improving their information system security measures. Work related to the government information system compliance audit this year have commenced in April.

- **Consultancy services**: The DPO launched a facilitation measure last year to assist B/Ds in procuring independent consultancy services to strengthen the management and security of government information systems, and to provide professional independent consultancy advice. As at May this year, the facilitation measure has completed 18 services for 11 information systems.

- **Supporting information security work for major events**: Concerning the major events held earlier, the DPO has strengthened real-time threat monitoring, intelligence sharing and attack and defence drill exercises to ensure the robust operation of relevant critical information systems.

- **Post-quantum cryptography technology assessment**: The powerful computational ability of quantum computing technology presents a risk to traditional encryption algorithms. Hence, by drawing reference to international mainstream strategies and recommendations from professional bodies, the DPO is formulating a comprehensive set of strategies and assessment mechanism to assist B/Ds in countering quantum threats and safeguard the information security defence line in the quantum era.

(II) Strengthening the dissemination of information security information within the Government

- **Safe Application of AI+ Governance**: The DPO continues to update the "Government IT Security Policy and Guidelines" to enhance the Government's overall cyber security defence capabilities. In response to the information security challenges posed by AI, the DPO has formulated the "Ethical Artificial Intelligence Framework" and the "Hong Kong Generative

Artificial Intelligence Technical and Application Guideline" to guide projects developing and applying AI technologies in identifying and managing potential risks and matters requiring attention associated with AI projects. In addition to the above guidelines, the DPO also issues security advisories based on the latest developments in information technology (IT), requiring B/Ds to consolidate the foundation of IT security, such as strengthening asset visibility, enforcing least-privilege principles, reducing attack surface, implementing risk-based patch management and comprehensive monitoring.

(III) Strengthening staff training and support

- **<u>Staff training</u>**: The DPO organises different types of training for government staff with the aim of enhancing their awareness of cyber security. As at July this year, the DPO and the Civil Service College (CSC) co-organised four thematic seminars, strengthening the core skills of the senior management (particularly senior directorates) of B/Ds in using digital technology and their capabilities in digital government management. In 2025-26, the DPO also arranged about 140 training courses related to the core skills in using digital technology for government staff, covering more than 8 100 participants. The DPO and the CSC will also launch a series of AI online courses this year, covering various areas such as basic AI concepts, related guidelines and usage principles, as well as safety and ethical awareness in using AI, thereby deepening government staff's foundational understanding of safe use of AI technology. A new round of the "Government-wide Phishing Drill Campaign" under the DPO will also be implemented, making use of new technologies such as AI to simulate phishing emails, thereby heightening government staff's awareness and ability to identify such frauds.

- **<u>Refresher courses</u>**: The DPO commissioned the HKIIT under the Vocational Training Council to offer "Certificate in Cybersecurity for the Public Sector" courses, aiming to enhance the professional capabilities of government staff in information security. As at May this year, more than 1 300 participants have completed the courses.

WAY FORWARD

9. The Government will continue to review and enhance existing efforts in safeguarding information security. In response to the risks arising from emerging technologies such as AI, the Government will consider formulating dedicated legislation and utilising various mechanisms to consolidate the cyber security defence ecosystem, supporting different types of organisations in strengthening their information security resilience and enhancing the overall cyber security protection capabilities of society.

ADVICE SOUGHT

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

Innovation, Technology and Industry Bureau
Digital Policy Office
July 2026

Annex I

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

Incident Category	June 2024 to May 2025		June 2025 to May 2026	
	Number of Cases	**%**	**Number of Cases**	**%**
Phishing (phishing websites)	8 549	57	9 764	62
Botnet (zombie computer)	3 561	24	2 396	15
Malicious Software (including ransomware)	1 372	9	1 288	8
Hacker Intrusion/ Web Defacement	10	<1	37	<1
Distributed Denial-of-Service (DDoS) Attacks	5	<1	1	<1
Others [1]	1 513	10	2 254	14
Total:	**15 010**	**100**	**15 740**	**100**

[1] Including online identity theft, data leakage, unauthorised system access, vulnerable system, etc.

Annex II

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

	2025	2026 (as of May)
Case Nature	**Number of Cases**	**Number of Cases**
Internet Deception	**27 528**	**9 807**
(i) Online Business Fraud	*13 102*	*5 246*
- *E-Shopping Fraud*	*12 505*	*3 973*
- *Payment Link Fraud*[2]	-	*1 026*
- *Credit Card Misuse*	*597*	*247*
(ii) Email Scam	*128*	*38*
(iii) E-Banking Fraud	*25*	*5*
(iv) Social Media Deception	*2 215*	*692*
(v) Miscellaneous Fraud (including online investment fraud and online employment fraud)	*10 965*	*2 817*
(vi) Phishing Scam	*1 093*	*1 009*
Internet Blackmail	**1 410**	**364**
(i) Naked Chat	*1 312*	*318*
(ii) Other Internet Blackmail	*98*	*46*
Misuse of Computer	**2 020**	**1 265**
(i) Unauthorised Access To Online Service Accounts	*1 968*	*1 250*
(ii) Hacking Activities	*52*	*15*
(iii) DDoS Attack	*0*	*0*
Others	**613**	**129**
Total (number of cases):	**31 571**	**11 565**
Monetary Loss (in $ million)	**6,321.2**	**2,074.5**

[2] Payment link fraud has been classified as a subcategory of technology crimes since 2026.