For discussion
on 14 October 2024

Legislative Council
Panel on Information Technology and Broadcasting

Work Related to Safeguarding and Promoting 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 and promoting information security.

OVERALL SITUATION OF INFORMATION AND CYBERSECURITY

2. Funded by the Government and established and operated by the Hong Kong Productivity Council (HKPC), the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) handled a total of 10 583 security incidents in the past year, representing an increase of approximately 39% from the previous year. The main categories of security incidents were phishing (6 141 cases) and botnets (2 663 cases) respectively. As compared with the previous year, the number of phishing cases increased by 83%, while the number of botnet cases dropped by about 27%. In addition, the number of cases in relation to malicious software (including ransomware) and web defacement both recorded an upward trend. The breakdown of statistics on these security incidents is at **Annex I**.

3. The Hong Kong Police Force (HKPF) recorded a total of 34 112 technology crimes in 2023, representing an increase of about 50% from 2022. The increase in the number of technology crimes was mainly due to the increase of cases in misuse of computer (e.g. unauthorised access to online service accounts) and internet deception (e.g. online investment fraud). For misuse of computer cases, the increase was mainly attributable to hijacking of instant messaging application accounts. In the first seven months of 2024, a total of 19 257 technology crimes were recorded, representing an increase of approximately 6% over the same

period last year. While unauthorised access to online service accounts remains the most significant, the increase in the overall number of technology crimes and the amount of money lost have both slowed down significantly when compared with the same period in the past two years. The breakdown of statistics on technology crimes is at **Annex II**.

4. In the case of personal data, the Office of the Privacy Commissioner for Personal Data (PCPD) handled 224 data breach incident notifications in the past year, which mainly involved hacker intrusions (85 cases), representing an increase of more than 200% as compared with the preceding year; loss of documents or portable devices (52 cases), representing an increase of 63% as compared with the preceding year; and accidental disclosure of personal data through email, post or fax (31 cases), representing an increase of 120% as compared with the preceding year.

PROMOTING INFORMATION SECURITY AT SOCIETY LEVEL

5. The Government has all along been committed to providing a secure and reliable cyber environment, and has been working closely with stakeholders such as the Hong Kong Internet Registration Corporation Limited (HKIRC) and HKCERT to provide relevant information and support to the general public to address the increasing information and cybersecurity risks. The related measures are as follows:

(I) Enhancing enterprises' capability in responding to cyberattacks

- Free website checking services and cybersecurity vulnerability testing: to enhance cybersecurity of local enterprises, the HKIRC has provided a free in-depth website security scanning service and telephone consultation for ".hk" users. In addition, the HKIRC launched "Healthy Web", a brand new website security checking service in 2023, and piloted the service in the education and social service sectors to proactively remind ".hk" users to take precautions against potential cyber risks. As at August 2024, the HKIRC has provided about 34 900 checking services to ".hk" users.

  Besides, the HKPF, the PCPD and the cybersecurity industry co-organised a three-month vulnerability discovery and remediation BugHunting Campaign from June to August 2024. A total of 153 enterprises and organisations participated in the campaign. Adopting a public-private partnership model, the campaign provides participating enterprises with free cybersecurity

vulnerability testing, cybersecurity reports and one-on-one professional cybersecurity consultation, so that enterprises can take appropriate measures to enhance their overall security protection level.

- Free online staff training: the HKIRC launched the "Cybersec Training Hub" in August 2022, which provided free online cybersecurity training to staff across various industries, raising the cybersecurity awareness and knowledge of enterprises and their staff. As at August this year, a total of about 219 400 people have attended the training.

- Cybersecurity information sharing: the Digital Policy Office (DPO) partners with the HKIRC to support the implementation of the cross-sector "Partnership Programme for Cyber Security Information Sharing" to promote the exchange of cybersecurity information among local enterprises and organisations (in particular SMEs). As at August this year, about 2 400 enterprises and organisations have joined the programme, covering different sectors including banking and finance, insurance, public utilities, transportation, medical care, telecommunications, innovation and technology (I&T), and education, etc.

- Cyber incidents hotline: the HKCERT provided a free 24-hour hotline for receiving security incident reports and offering advice on incident response and recovery.

(II) Stepping up public education

- Promoting cybersecurity: the DPO is committed to promoting and raising the cybersecurity awareness of the community over the years. To echo the "China Cybersecurity Week" activities, the DPO collaborated with industry players to organise the "2024 Cybersecurity Awareness Campaign" this year. Themed "Together, We Create a Safe Cyberworld", activities such as Hong Kong side-forum, tram body design contest, exhibitions, fun day, technical seminars and relevant learning resources were organised to convey cybersecurity and national security messages to the public. The DPO also updates the "InfoSec" and "Cyber Security Information Portal" thematic websites from time to time, including updating educational videos and quizzes to introduce the general public with the latest cybersecurity information, as well as how to prevent cyberattacks.

- Protection of personal data: the PCPD proactively promotes measures 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, which includes how to safely utilise portable devices, 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 heighten public awareness against fraud. Targeting frauds committed through hijacking of instant messaging application accounts, the HKPF has enhanced publicity via various channels such as their "CyberDefender" website and Facebook, and organised a large-scale press conference in which fraudsters' modus operandi of hijacking instant messaging application accounts was demonstrated to advise the public on ways to prevent their accounts from being hijacked. The HKPF has also promptly alerted telecommunications service providers to intercept the relevant websites, and requested the search engines and overseas authorities concerned to remove the false WhatsApp website advertisements.

  In addition, the HKPF launched "Scameter" and relevant mobile application, issuing more than 650 000 alerts on frauds and cyber security risks. 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 will be expanded to cover Automatic Teller Machines in the first quarter of 2025 to provide full coverage and better protect the public.

(III) Promoting cross-territory cooperation

- Regular contact and exchange: the Government Computer Emergency Response Team Hong Kong maintains close contacts with other regional computer emergency response teams (CERT) by joining the international CERT Coordination Centre, the Forum of Incident Response and Security Teams, and the Asia Pacific Computer Emergency Response Team (APCERT), and participated in technical exchanges organised by various

organistions, including the regular APCERT incident response drill.

- Symposiums: in December last year, the DPO collaborated with the HKIRC to organise the "Cybersecurity Symposium 2023", which brought together top-notch cybersecurity experts from Hong Kong and the Mainland to jointly explore how to strengthen Hong Kong's overall defence and resilience capabilities against cyberattacks. The Government has also actively participated in the annual "World Internet Conference Wuzhen Summit" organised by the Cyberspace Administration of China, and delivered a keynote speech in the Summit last year, sharing the development and implementation of cybersecurity in Hong Kong.

- Memorandum of Understanding: in September 2024, the DPO signed a "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 will strengthen cooperation in the aspects of technological exchange, information sharing, and emergency response measures among Hong Kong, Guangdong Province and Macao SAR, and support for building a safe digital Greater Bay Area.

(IV) Making legislation and guidelines

- Computer-system security of critical infrastructures: to enhance protection of computer-system security of critical infrastructures, and promote the establishment of good preventive management systems by operators of critical infrastructures, the Security Bureau (SB) has consulted the LegCo Panel on Security on the proposed legislative framework in July this year, and consulted the trade again. The SB has submitted the consultation report to the LegCo Panel on Security, and plans to introduce the Bill into LegCo within this year.

- Data centre infrastructure security: the DPO is working with the industry to develop "Practice Guides on Data Centre Security", covering the management, design, operation and maintenance of data centre security, providing practical guidelines for reference, with a view to enhancing the security of data centre infrastructure in Hong Kong. The DPO expects to promulgate the guides by the end of this year.

STRENGTHENING INFORMATION SECURITY IN THE GOVERNMENT

6. The Government has all along adopted a multi-pronged approach to strengthen the information and cybersecurity of policy bureaux / departments (B/Ds). The related policy and measures are as follows:

(I) Formulating and updating policies and guidelines

- Information security policy: the Government has formulated and updated from time to time the comprehensive "Government Information Technology (IT) Security Policy and Guidelines" ("Policy and Guidelines"), which covers the management framework, policies and technical measures, for adherence by all B/Ds. The updated "Policy and Guidelines" issued in April this year further strengthened different areas of information security control measures and enhanced the protection of government IT systems in tiers, with a view to ensuring security of the government IT systems and data more effectively. The "Policy Statement on Facilitating Data Flow and Safeguarding Data Security in Hong Kong" published by the Innovation, Technology & Industry Bureau and DPO in December 2023 also sets out specific action items to enhance safeguards for data security and planning of facilities in Hong Kong.

- Practice guides: the DPO developed a comprehensive set of guidelines that covers various aspects of information security, including the "Practice Guide for Cloud Computing Security" which provided practical guidance and reference for the secure adoption of cloud computing technology in the Government. At the same time, all B/Ds are required to conduct a comprehensive review of existing information security measures to ensure that all systems and users under their purview strictly comply with the relevant requirements, including no storage of sensitive and personal data in public cloud platform to ensure proper data protection. The updated "Practice Guide for Mobile Security" issued in June this year also strengthened the monitoring and security of mobile devices used by government staff, in order to effectively manage the risk of sensitive government data leakage.

(II) Strengthening staff training and support

- Staff training: the DPO organises seminars and solution sharing sessions from time to time to enable government staff to understand the latest cybersecurity trends and preventive measures, thereby enhancing their information security knowledge. As at September this year, the number of participants exceeded 7 100, representing an increase of about 173% as compared with the previous year. The DPO will continue to enhance training to deepen government staff's understanding and preparedness on information and cybersecurity.

- Refresher courses: the DPO is organising a "Cybersecurity Certificate Training Scheme" with the "Hong Kong Institute of Information Technology" (HKIIT) under the Vocational Training Council (VTC) to offer courses for relevant government staff to enhance their information security professional skills.

- Anti-phishing campaigns: the DPO will launch a new round of "Government-wide Phishing Drill Campaign" in 2025, making use of new technologies such as artificial intelligence to simulate phishing emails to deepen the awareness of government staff on phishing.

(III) Improving project governance and security of IT systems of the Government and public bodies

7. To enhance the IT security of B/Ds and public bodies, the Government has implemented several improvement measures in August this year, which require B/Ds and public bodies under their purview to strengthen the project governance and security of IT systems. The relevant key measures include:

Strengthening supervisory responsibility

- Role of senior officials: all B/Ds and related public bodies should assign senior directorate officers to be responsible for project governance of important IT systems, covering the supervision and information security work throughout the entire system development and implementation cycle, so as to identify and deal with security risks of IT systems at early stage and ensure the secure and reliable delivery of services by the systems.

- Incident handling mechanism of electronic systems: the security incident handling mechanism for important government or public body IT systems has been enhanced to clearly define the post-incident handling procedures and follow-up work.

Enhancing system security and stability

- Additional tests, assessments and audits: all B/Ds and public bodies must arrange additional stress test and security test by an independent third party before rollout of their IT systems, establish a standing monitoring mechanism on the system and conduct self-assessments such as security risk assessment and audit, privacy impact assessment, regular system checking and penetration testing during the normal production stage. The DPO will provide appropriate technical advice, guidelines, best practice guides and other relevant information, e.g. specifications for stress test and security test, risk factors associated with the setting of test parameters, etc.

Comprehensive and standardised IT system checking and defence

- System health check and compliance audit: the DPO will conduct regular and continuous health checks and penetration tests on government public-facing IT systems, as well as security compliance audits under a risk-based approach.

- Cybersecurity attack and defence drill: the DPO will organise annual cybersecurity attack and defence drill, during which B/Ds and organisations will form "blue teams" to defend against simulated hacker attacks launched by "red teams" comprising cybersecurity experts and industry players, so as to test the response and resilience capabilities of systems in the event of cyberattacks. Through the drill, it is anticipated that B/Ds and public bodies can improve their technique, experience and overall defence capabilities in identifying and responding to cyberattacks, thereby fortifying their defence line. The first real-life cybersecurity attack and defence drill will be held in November this year.

HUMAN RESOURCES DEVELOPMENT

Primary and secondary levels

8. The Government attaches importance to nurturing information literacy among students in the digital technology era. The Education Bureau (EDB) provides schools with the "Information Literacy for Hong Kong Students" Learning Framework to teach students about the importance of information and cyber security, as well as personal data privacy protection. At the same time, a series of related teacher training courses are organised and relevant teaching resources are developed.

9. Beyond the regular curriculum, the DPO implements the "IT Innovation Lab in Secondary Schools" and "Knowing More About IT" programmes, subsidising secondary and primary schools respectively to organise extra-curricular activities related to information technology, including cybersecurity related courses, workshops and competitions, etc. As at September this year, nearly 1 000 schools have organised about 5 500 activities under the two programmes, which included cybersecurity related extra-curricular activities such as cybersecurity introductory courses and technical workshops.

Post-secondary institution 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 number of places. 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 including computer science (covering cybersecurity) to meet Hong Kong's social and economic needs. In 2024/25 academic year, SSSDP covers five undergraduate and two sub-degree programmes in the computer science discipline, involving a total of 405 subsidised places.

11. Furthermore, the VTC newly established the HKIIT in November 2023, which focuses on providing IT and other related technology programmes, including Higher Diploma (HD) in Telecommunications and Networking, HD in Cybersecurity, with a view to strengthening the IT capacity of Hong Kong, responding to the manpower demand of the sector, and promoting Hong Kong's future development.

Retraining, continuing education and vocational training

12. On local manpower training, the Employees Retraining Board currently offers over 700 regular training courses for eligible persons straddling across 28 industries and generic skills, including courses in the cybersecurity and management field. Hong Kong residents aged over 18 or above may also make use of the Continuing Education Fund to enroll in courses relating to computer science and information technology.

13. Moreover, the HKPF, the DPO and the HKCERT jointly organised the Cyber Security Professionals Awards again in 2023 to recognise and motivate outstanding cybersecurity managers and practitioners, and provide a platform for experience sharing to enhance their professional capabilities, with a view to building an innovative and ever-improving cyber ecosystem. The number of participating sectors has also been increased from five last round to eight, covering new sectors such as Cyber Security Audit & Consulting, Cybersecurity Education & Training, and Cybersecurity Startups and Small and Medium Enterprises.

WAY FORWARD

14. The Government will continue to enhance the cybersecurity awareness and defensive capability of the community on all fronts, and strengthen the security of IT systems within the Government and public bodies, with a view to building Hong Kong into a safer and more reliable smart city.

ADVICE SOUGHT

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

Innovation, Technology and Industry Bureau
Digital Policy Office
October 2024

Annex I

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

Incident Category	Same period in previous year (September 2022 - August 2023)		In the past year (September 2023 - August 2024)		
	Number of cases	%	Number of cases	%	Compared with same period in previous year
Phishing (phishing websites)	3 350	44	6 141	58	+83%
Botnet (zombie computer)	3 671	48	2 663	25	-27%
Malicious Software (including ransomware)	136	2	618	6	+354%
Hacker Intrusion/Web Defacement	15	<1	19	<1	+25%
Distributed Denial-of-Service (DDoS) Attacks	2	<1	2	<1	0
Others [1]	422	6	1 140	11	+170%
Total:	**7 596**	**100**	**10 583**	**100**	**+39%**

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

Annex II

Statistics on Technology-related Crimes Handled by The Hong Kong Police Force and the Resulting Monetary Loss

	2022	2023		2024 (Up to July)
Case Nature	**Number of Cases**	**Number of Cases**	**Compared with 2022**	**Number of Cases**
Internet Deception	**19 599**	**27 314**	**+39.4%**	**14 898**
(i) Online Business Fraud	*9 279*	*9 883*	*+6.5%*	*6 612*
- E-Shopping Fraud	*8 735*	*8 950*	*+2.5%*	*6 280*
- Credit Card Misuse	*544*	*933*	*+71.5%*	*332*
(ii) Email Scam	*391*	*208*	*-46.8%*	*134*
(iii) E-Banking Fraud	*7*	*16*	*+128.6%*	*15*
(iv) Social Media Deception	*3 605*	*3 372*	*-6.5%*	*1 829*
(v) Miscellaneous Fraud (include Online Investment Fraud)	*6 317*	*9 513*	*+50.6%*	*4 849*
(vi) Phishing Scam [2]	*-*	*4 322*	*-*	*1 459*
Internet Blackmail	**1 557**	**2 428**	**+55.9%**	**1 437**
(i) Naked Chat	*1 402*	*2 117*	*+51%*	*1 365*
(ii) Other Internet Blackmail	*155*	*311*	*+100.6%*	*72*
Misuse of Computer	**192**	**3 471**	**+1 707.8%**	**2 428**
(i) Unauthorised Access To Online Service Accounts	*168*	*3 434*	*+1 944%*	*2 389*
(ii) Hacking Activities	*24*	*37*	*+54.2%*	*37*
(iii) DDoS Attack	*0*	*0*	*-*	*2*
Others	**1 449**	**899**	**-38%**	**494**
Total (number of cases):	**22 797**	**34 112**	**+49.6%**	**19 257**
Monetary Loss (in $ million)	**3,215.4**	**5,496.8**	**+71%**	**3,075.1**

[2] "Phishing Scam" is newly captured as a technology-related crime since January 2023.