The 11th ASEAN – China Prosecutors-General Conference
Enhancing Capabilities and Cooperation in Addressing Cybercrime

"*A keynote address of about 15 minutes on your country's efforts in combatting cybercrime and sharing of experiences*"

Cybercrime is a growing problem across jurisdictions. The advent of the Internet has given rise to the advent of cybercrime in different forms. In Hong Kong, the number of cybercrime cases increased from 2,206 in 2011 to 5,939 in 2016, and the financial losses occasioned by cybercrime also recorded a rapid upsurge, dramatically from HK$149 million in 2011 to HK$2,301 million in 2016[1] [see Annex A]. Common cybercrime include ransomware attack, social media deception, e-banking fraud, email scam, online social networking traps and online blackmail[2]. Analyzed by type, online business fraud was the largest category of cybercrime in Hong Kong, accounting for 27% of the overall cases in 2016, followed by social media deception at 19%[3].

In Hong Kong, the Computer Crimes Ordinance was enacted in 1993 to amend various ordinance including the Crimes Ordinance (Cap 200) to counter different forms of cybercrime.. The main statutory provisions that deal with cybercrime under the Crimes Ordinance include *inter alia* (1) access to a computer with criminal or dishonest intent[4], and (2) criminal damage[5] relating to the misuse of a computer.

An example of the case of access to a computer with criminal or dishonest intent is the landmark case of ***HKSAR v Tsun Shui Lun*** [1999] 3 HKLRD 215. The defendant Tsun was a technical assistant to a radiologist of a hospital. He obtained unauthorized access to the computer system of the hospital that contained the medical records of the then Secretary for Justice, printed out a copy of the patient's medical report and took it home to show to his wife. On the next day, Tsun accessed the computer system again, printed out another

[1]https://www.legco.gov.hk/research-publications/english/1718issh06-cyber-security-in-hong-kong-20171220-e.pdf
[2] https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/
[3] Ibid, n1
[4] Section 161 of Crimes Ordinance, Cap. 200
[5] Sections 59 and 60 of Crimes Ordinance, Cap. 200

copy and faxed it to the press. He was charged two counts of "access to a computer with a view to dishonest gain for himself". He was convicted at the first instance and on appeal, the Court laid down the following principles:

(1) The section catches acts preparatory to the commission of a crime or fraud, though not restricted to these acts. The Court gave a few examples:

(a) a businessman who wants to acquire information about his competitors in order to enable himself to have an advantage over them;

(b) a disgruntled employee who wants to ruin his employer's business by revealing his employer's trade secrets to others;

(c) an ex-employee who wants to obtain a list of his former employer's customers in order to solicit business from them;

(d) a dissatisfied bank officer who wants to erase the bank's records from the computer in order to cause confusion or to irritate the bank's customers

(2) As to the word "gain", the Court noted that:

(a) it is not confined to financial or proprietary benefits, but is wide enough to cover intangible benefits;

(b) it can be a transient as opposed to permanent benefit;

(c) the keeping of what one has or the getting of what one has not is also regarded as a gain;

(d) it covers a benefit or an advantage – it need not be something which can be utilized or used.

These principles have then been consistently applied.

As to criminal damage relating to misuse of computer, a typical example

is in ***HKSAR v Chu Tsun-wai*** HCMA 454 of 2016, the defendant Chu was convicted of one count of criminal damage for having launched a Distributed Denial of Service ("DDos") attack on the server of a bank by making 6,652 HTTP requests in 16 seconds, out of a total of 504,592 requests made to the bank's server in about an hour, in response to an appeal made by an international hacker organization called "Anonymous Asia". On appeal the defendant argued that the facts did not constitute the offence of criminal damage because the attacks did not affect the operation of the server of the bank, although there was evidence that some bandwidth of the server was being occupied. The appeal was dismissed but the defendant has now applied for leave to appeal to the Court of Final Appeal (FAMC 35 of 2018).

The amendments are broadly adequate to deal with illicit acts such as hacking, ransomware attack or misuse of computer data. Other legislations also deal with different kinds of computer related crimes, such as disclosing personal data without consent of data subject with intent to obtain gain or to cause loss under the Personal Data (Privacy) Ordinance, or forgery, false accounting and making false entry in bank book under the Crimes Ordinance and the Theft Ordinance, which cover crimes perpetrated in connection with data or information recorded or stored by electronic means.

In response to the significant increase in cybercrime, the Prosecutions Division of the Department of Justice of the HKSAR has established a computer crime section within the Commercial Crime Unit since 2000. A dedicated Cybercrime Section was subsequently established in 2012 to foster closer working relationship with our counterparts in the law enforcement agencies. Over the years the team has been responsible for providing expert legal advice on cybercrime, preventing technology crime and conducting related prosecutions. It also carries out research and training to prosecutors to deal with cases involving cybercrime. To enhance its effectiveness, the team liaises regularly with local law enforcement agencies and international prosecution agencies. Counsel of the team also attend local and overseas conferences and training courses in order to keep abreast of the latest developments in tackling cybercrime.

On the part of the police, a Computer Crime Section ("CCS") has been set up within the Commercial Crime Bureau of the Hong Kong Police Force

since 1993 for the investigation of computer related crimes[6]. The 18-member CCS was responsible for the centralized forensic examination of computer evidence involved in crimes that were investigated by other Police formations. A restructuring was conducted in 2001 to expand the CCS into a Technology Crime Division ("TCD") within the Commercial Crime Bureau, followed by a further expansion of TCD by doubling its manpower in 2011. The Hong Kong Police Force established the Cyber Security and Technology Crime Bureau ("CSTCB") in 2015 as a bureau within the Force with a view to strengthen its capability in detecting syndicated and highly sophisticated computer crimes, as well as enhancing response capability against major cyber security incidents or massive cyber attacks. The establishment of the CSTCB in 2016-17 comprised 238 posts[7], representing a significant increase in the manpower and capability compared with its predecessors.

Rapid technological advancement means that we have to race against time in combating cybercrime. Existing legislations may not always be sufficient in specifically addressing issues raised in courts. For example, there is no definition of a computer in our legislation, although recent cases have ruled that smartphones are "computers" under the Crimes Ordinance. In the case of ***SJ v WONG Ka-yip Ken*** HCMA 77 of 2013, the respondent was caught taking video with his smartphone inside a female toilet. He was charged with "obtaining access to a computer with a view to dishonest gain", contrary to s161(1)(c) of the Crimes Ordinance. The trial magistrate found that the smartphone was not a "computer" stated in s161, and the Secretary for Justice appealed by way of case stated against the decision and asked for a conviction. In overturning the magistrate's decision and convicting the respondent, the Appellate Court held that the term "computer" under s 161 of the Crimes Ordinance should be construed according to its dictionary meaning which reads "*an electronic device which is capable of receiving information in a particular form and of performing a sequence of operations in accordance with a predetermined but variable set of procedural instructions to produce a result in the form of information or signals*". This also accorded with the internationally accepted definition of "computer" as a device for storing, processing and retrieving electronic data and came in line with the provisions and judgments of other countries. The Court also took the view that the Legislative Council did not define "computer"

[6] Report of the Inter-departmental Working Group on Computer Related Crime, September 2000
https://www.hkispa.org.hk/pdf/ComputerRelatedCrime.pdf
[7] https://www.legco.gov.hk/yr15-16/english/fc/esc/papers/e16-17e.pdf

under s 161 of the Crime Ordinance because science and technology were fast-developing, the definition of "computer" was broad and ever-evolving and could never be exhaustive. It should be noted that under the current regime the taking of photographs or video recording by way of smartphone for sexual purpose may constitute an offence under s161 of the Crimes Ordinance, but the Law Reform Commission in Hong Kong is now reviewing the laws and proposed to create a specific offence of voyeurism involving visual recording for a sexual purpose.

Another example of cases which gives rise to a debate before the Court of Final Appeal is the case of ***HKSAR v CHAN Yau-hei*** FACC 3/2013. The issue was whether the internet or cyberspace is a public place for the purpose of the offence of outraging public decency. In that case the appellant posted a message on a website discussion forum suggesting the planting of a bomb. It was held by the Court of Final Appeal that the public element of the offence of outraging public decency requires the act to be committed in a physical and tangible place, and the internet is not a place in any physical or actual sense. The internet is only a medium but not a place for the purposes of the offence.

The HKSAR Government attaches great importance to combating cybercrime. However, since cyber security and technology crimes are fast evolving and transcend traditional jurisdictional boundaries, the prosecution is always facing an enormous challenge. The enforcement of cybersecurity laws in relation to cross-border matters is one best example. In 2002, the Government introduced the Criminal Jurisdiction Ordinance to address the jurisdictional problems associated with cross-border related crimes. However, it has yet come into operation to enable Hong Kong courts to exercise jurisdiction over computer-related crimes committed or planned outside Hong Kong. Other cross-border issues include how to establish in evidence the true identity of the offender in the absence of admissions given the evidential gap between true identity of the offender and their pseudo-identity in the cyber world, and how to effectively obtain necessary admissible evidence from overseas jurisdictions with different data privacy policies especially when mutual legal assistance is deemed inappropriate. To tackle all these issues, it requires the collaboration and concerted efforts between different government departments, law enforcement agencies and stakeholders, both within and across jurisdictions. The DoJ will continue to cooperate with our counterparts, both local and overseas, in order to effectively combat cybercrime.

Prosecutions Division
Department of Justice, HKSAR
July 2018

Information Technology and Broadcasting

Research Office
Legislative Council Secretariat

Statistical Highlights

ISSH06/17-18

Cyber security in Hong Kong

Figure 1 —Total financial losses of cybercrime

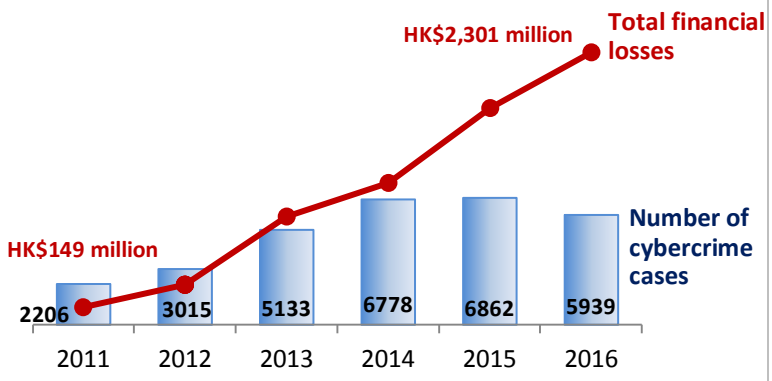
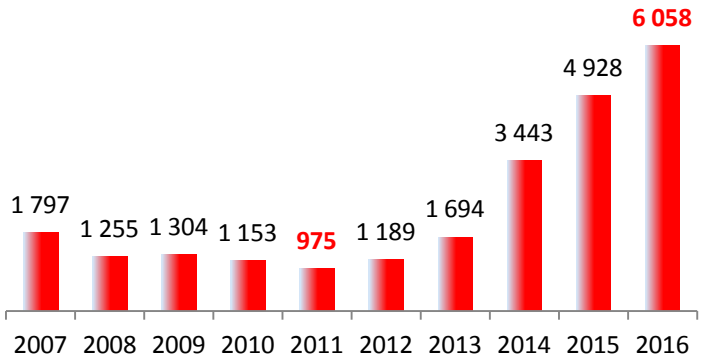


Figure 2 — Cybercrime cases by type

	2011	2013	2015	2016
Online business fraud	888	1 449	1 911	**1 602**
Social media deception	N.A.	261	1 422	**1 150**
Unauthorized access to computer	567	1 986	1 223	**1 107**
Naked chat-related blackmail	N.A.	477	1 098	697
Others	751	960	1 208	1 383
Total	2 206	5 133	6 862	5 939

Figure 3 — Number of IT security incidents*



Note: (*) Cases reported to Hong Kong Computer Emergency Response Team Coordination Centre.

Highlights

- In view of a 207% upsurge in cybercrime in just three years till 2014, the Police established the Cyber Security and Technology Crime Bureau in 2015. While it helped lower cybercrime cases by 13.5% in 2016, total financial losses increased visibly further by 26% to reach a new high at HK$2.3 billion (**Figure 1**). Average financial loss per case even surged by 45% to reach a high at HK$387,400 last year.

- Analysed by type, online business fraud was the largest category of cybercrime in Hong Kong, accounting for 27% of the overall cases in 2016, followed by social media deception at 19% (**Figure 2**). Although unauthorized access to computer was the third largest category (with a share of 19%), it was the largest contributor to the recent surge in the financial loss. In 2016, the financial losses arising from corporate-level email scams under the category of unauthorized access to computers surged by 363% to HK$1.8 billion.

- Separately, there has been a noticeable increase in security risk disrupting confidentiality, integrity and availability of computer systems. The number of information technology ("IT") security incidents has increased by 23% to 6 058 cases in the single year of 2016, and by a total of 521% during 2011-2016 (**Figure 3**).

Figure 4 — Types of IT security incidents in 2015-2016

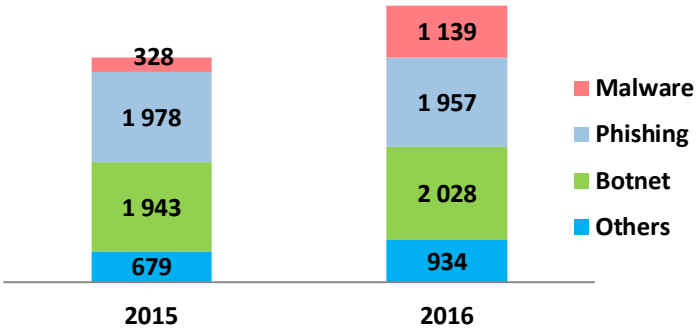


Figure 5 — Number of IT security employees by sector in 2016

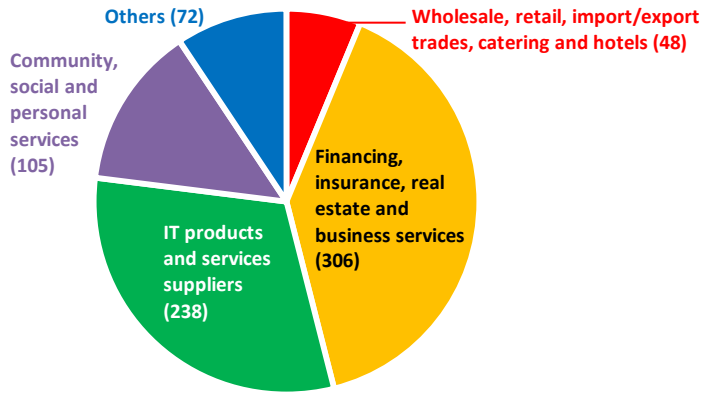
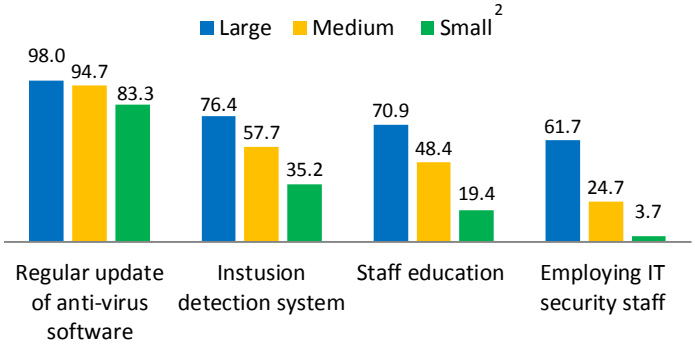


Figure 6 — Selected types of IT security measures adopted by business in 2015 (%)[1]



Notes: (1) % of establishments having adopted IT security measures.
(2) Small establishments are those with nine employees or below, while medium-sized establishments are those with 10-99 employees in manufacturing sector or 10-49 employees in service sectors.

Highlights

- Amongst all IT security risks in 2016, Botnet (i.e. networks of infected computers controlled by hackers) and Phishing (i.e. scam messages to obtain sensitive information) took up 66% of cases (**Figure 4**). More recently, there have been growing concerns over increased malware attacks (i.e. intrusive software causing harm to computers), with a 247% increase to 1 139 cases in 2016. Amongst these malware attacks, 27% involved ransomware (i.e. malware threatening victims to publish their data or block their access to their data unless a ransom is paid).

- In 2016, there were just 769 IT employees specializing in IT security in Hong Kong, representing only 0.9% of all IT employees and suggesting an underestimation of IT security risks in the local community. As the majority (71%) of these IT security specialists were employed in IT, financial and business-related sectors, there are concerns that IT security manpower support to other sectors is rather limited (**Figure 5**).

- By and large, small and medium-sized establishments are more vulnerable to cyber security threats due to resource constraints. According to a survey on business establishments with IT security measures, only 4% of small establishments and 25% of medium-sized establishments had IT security staff, far less than that of large establishments (62%) (**Figure 6**).

Data sources: Latest figures from Census and Statistics Department, Fight Crime Committee, Hong Kong Computer Emergency Response Team Coordination Centre, Hong Kong Police Force and Vocational Training Council.

Research Office
Information Services Division
Legislative Council Secretariat
20 December 2017
Tel: 2871 2139