

**立法會**  
**Legislative Council**

LC Paper No. CB(1)1329/18-19  
(These minutes have been seen  
by the Administration)

Ref : CB2/PL/CA+CB1/PL/ITB+CB2/PL/SE

**Panel on Constitutional Affairs,  
Panel on Information Technology and Broadcasting  
and Panel on Security**

**Minutes of joint meeting  
held on Wednesday, 14 November 2018, at 8:30 am  
in Conference Room 2 of the Legislative Council Complex**

**Members present** : Members of the Panel on Constitutional Affairs

- \* Hon CHEUNG Kwok-kwan, JP (Chairman)
- Hon LUK Chung-hung, JP (Deputy Chairman)
- \* Hon Jeffrey LAM Kin-fung, GBS, JP
- \* Hon Starry LEE Wai-king, SBS, JP
- #\* Hon CHAN Kin-por, GBS, JP
- \* Dr Hon Priscilla LEUNG Mei-fun, SBS, JP
- # Hon Mrs Regina IP LAU Suk-ye, GBS, JP
- #\* Hon Paul TSE Wai-chun, JP
- #\* Hon Claudia MO
- #\* Hon MA Fung-kwok, SBS, JP
- #\* Hon CHAN Chi-chuen
- \* Hon Alice MAK Mei-kuen, BBS, JP
- #\* Hon Christopher CHEUNG Wah-fung, SBS, JP
- Hon IP Kin-yuen
- # Hon Martin LIAO Cheung-kong, SBS, JP
- Dr Hon CHIANG Lai-wan, SBS, JP
- #\* Hon CHUNG Kwok-pan
- #\* Hon Alvin YEUNG
- #\* Hon CHU Hoi-dick
- \* Hon Jimmy NG Wing-ka, JP
- \* Hon LAM Cheuk-ting
- \* Hon Holden CHOW Ho-ding

- Hon Tanya CHAN  
#\* Hon HUI Chi-fung  
Hon LAU Kwok-fan, MH  
Hon Kenneth LAU Ip-keung, BBS, MH, JP  
\* Dr Hon CHENG Chung-tai  
\* Hon AU Nok-hin

Members of the Panel on Information Technology  
and Broadcasting

- \* Dr Hon Elizabeth QUAT, BBS, JP (Chairman)  
^\* Hon Charles Peter MOK, JP (Deputy Chairman)  
\* Hon YIU Si-wing, BBS  
\* Hon YUNG Hoi-yan  
\* Hon CHAN Chun-ying, JP

Members of the Panel on Security

- ^ Hon CHAN Hak-kan, BBS, JP (Chairman)  
# Hon James TO Kun-sun (Deputy Chairman)  
Hon Michael TIEN Puk-sun, BBS, JP  
Hon Frankie YICK Chi-ming, SBS, JP  
Hon CHAN Han-pan, BBS, JP  
Hon LEUNG Che-cheung, SBS, MH, JP  
Hon Kenneth LEUNG  
Hon POON Siu-ping, BBS, MH  
Hon SHIU Ka-chun  
Hon Tony TSE Wai-chuen, BBS

- Members absent** : Members of the Panel on Constitutional Affairs  
# Hon WONG Ting-kwong, GBS, JP  
\* Hon WONG Kwok-kin, SBS, JP  
Hon Steven HO Chun-yin, BBS  
\* Hon Dennis KWOK Wing-hang  
Dr Hon Helena WONG Pik-wan  
# Ir Dr Hon LO Wai-kwok, SBS, MH, JP

Members of the Panel on Security

- Hon KWOK Wai-keung, JP  
Dr Hon Fernando CHEUNG Chiu-hung  
Dr Hon Junius HO Kwan-yiu, JP

**Members attending** : Dr Hon KWOK Ka-ki  
Hon HO Kai-ming  
Hon Jeremy TAM Man-ho

(^ Also members of the Panel on Constitutional Affairs)

(# Also members of the Panel on Information Technology and Broadcasting)

(\* Also members of the Panel on Security)

**Public officers attending** : Agenda item II

The Administration

Mr Patrick NIP Tak-kuen, JP  
Secretary for Constitutional and Mainland Affairs

Miss Rosanna LAW Shuk-pui, JP  
Deputy Secretary for Constitutional and Mainland Affairs

Mr Jason PUN Si-keung  
Assistant Government Chief Information Officer  
(Cyber Security and Digital Identity), Office of the  
Government Chief Information Officer

Mr Andrew TSANG Yue-tung  
Principal Assistant Secretary for Security

Mr Joe CHAN Tung  
Chief Superintendent of Cyber Security and  
Technology Crime Bureau, Hong Kong Police  
Force

The Office of the Privacy Commissioner for Personal Data

Mr Stephen WONG Kai-yi  
Privacy Commissioner for Personal Data

Ms Raina YEUNG Sau-ling  
Assistant Privacy Commissioner for Personal Data

Ms Joyce LAI Chi-man  
Head of Compliance and Enquiries

Cathay Pacific Airways

Mr John SLOSAR  
Chairman

Mr Rupert HOGG  
Chief Executive Officer

Mr Paul LOO  
Chief Customer and Commercial Officer

Ms Kerry PEIRSE  
General Manager, IT Infrastructure and Operations

**Clerk in attendance** : Mr Daniel SIN  
Chief Council Secretary (4)3

**Staff in attendance** : Mr Ambrose LEUNG  
Senior Council Secretary (4)3

Ms Peggy CHUNG  
Council Secretary (4)3

Miss Emma CHEUNG  
Senior Legislative Assistant (4)3

Ms Cynthia TAM  
Legislative Assistant (4)3

Ms Yvonna HO  
Clerical Assistant (4)3

---

Action

**I. Election of Chairman**

Mr CHEUNG Kwok-kwan, Chairman of the Panel on Constitutional Affairs ("CA Panel"), said that Dr Elizabeth QUAT, Chairman of the Panel on Information Technology and Broadcasting and Mr CHAN Hak-kan, Chairman of the Panel on Security, had agreed that he should preside over the joint Panel meeting. Members also agreed that Mr CHEUNG would conduct the joint meeting in accordance with paragraph 22(k) of the House Rules.

**II. The incident of leakage of passengers' personal data by Cathay Pacific Airways and issues relating to protection of personal data and cyber security**

- (LC Paper No. CB(2)222/18-19(01) -- Paper provided by the Administration
- LC Paper No. CB(2)222/18-19(02) -- Paper provided by Cathay Pacific Airways
- LC Paper No. CB(4)166/18-19(01) -- Letter dated 2 November 2018 from Hon Charles Peter MOK to Chairman of Panel on Information Technology and Broadcasting
- LC Paper No. CB(2)230/18-19(01) -- Cathay Pacific Airways' response to Hon Charles Peter MOK's letter dated 2 November 2018 to Chairman of Panel on Information Technology and Broadcasting
- LC Paper No. CB(4)205/18-19(01) -- Letter dated 13 November 2018 from Dr Hon Elizabeth QUAT to Panel on Information Technology and Broadcasting
- LC Paper No. CB(2)158/18-19(01) -- Letter dated 25 October 2018 from Hon LUK Chung-hung to Chairman of Constitutional Affairs Panel
- LC Paper No. CB(2)158/18-19(02) -- Letter dated 25 October 2018 from Dr Hon Elizabeth QUAT to Chairman of Constitutional Affairs Panel
- LC Paper No. CB(2)158/18-19(03) -- Letter dated 25 October 2018 from Hon LAM Cheuk-ting to Chairman of Constitutional Affairs Panel

LC Paper No. CB(2)222/18-19(03) -- Background brief prepared by the Legislative Council Secretariat)

Presentation by the Administration

2. At the invitation of the Chairman, Secretary for Constitutional and Mainland Affairs ("SCMA"), Privacy Commissioner for Personal Data ("PCPD") and Chairman, Cathay Pacific Airways briefed members on the incident of leakage of passengers' personal data by Cathay Pacific Airways ("CX") and issues relating to protection of personal data and cyber security. Details were set out in the LC Paper No. CB(2)222/18-19(01) and CB(2)222/18-19(02).

*(Post-meeting note: The speaking notes were issued to members by e-mail via LC Paper Nos. CB(4)216/18-19(02) (SCMA) and CB(4)216/18-19(03) (CX) on 15 November 2018 and CB(4)226/18-19(01) (PCPD) on 19 November 2018.)*

Discussion

*Delay in Cathay's disclosure of the incident*

3. Mr CHAN Hak-kan criticized CX for not having protected passengers' personal data. He also criticized the company for failing to report the matter to the Police and to inform the affected passengers at the earliest opportunity after having discovered that there had been a security breach of the system. Ms Claudia MO, Mr LAU Kwok-fan, Dr Elizabeth QUAT, Mr AU Nok-hin and Dr KWOK Ka-ki made similar comments. In particular, Ms MO accused CX of covering up the incident.

4. Mr CHAN Hak-kan and Ms YUNG Hoi-yan queried whether the delay in disclosing the incident was due to problems of the company's internal communication. Mr Charles Peter MOK commented that the disclosed information was unclear and fragmented. Mr CHAN Chi-chuen criticized CX for not notifying their customers at the earliest opportunity. Mr LAU Kwok-fan, Mr James TO Kun-sun and Ms Alice MAK Mei-kuen pointed out that victims of the breach could have responded to the data leakage more timely should CX announced the incident earlier. Upon the request of Mr Tony TSE Wai-chuen, Chief Superintendent of Cyber Security and Technology Crime Bureau, Hong Kong Police Force also confirmed that the earlier cybercrimes were reported, the better.

5. The Chief Executive Officer of CX ("CEO, CX") apologized for the delay in making the announcement. He explained that once the cyber-attacks were discovered, the company had immediately engaged external cyber forensic experts to help contain the attacks and to carry out measures to prevent further damages from the attacks. CEO, CX said that it had taken longer than expected to carry out investigation and containment measures and to take remedial actions. He added that time was also needed to identify which data had been accessed and to determine how the passengers were affected as much of the data was not stored in formats readable by external parties.

6. Chairman, CX and CEO, CX maintained that there was never an intention to cover up the incident, and the company had tried to provide detailed information to help passengers assess to what risks they were exposed.

#### *Scope of the incident*

7. Mr Jeffrey LAM Kin-fung asked whether CX's other administrative information had been hacked and how the company could ensure that passengers' financial information was not leaked. General Manager, IT Infrastructure and Operations of CX said that after a full forensic review of the environment, the company was informed that no financial information or information from their human resources services was compromised. Mr CHAN Chi-chuen commented that CX's announcement about the incident did not clearly state whether the cyber-attack at the company's database was still on-going, or whether there was any subsequent data leakage since March 2018. Mr YIU Si-wing asked whether passengers' personal data were safe if they had not received any notification from the company in relation to the incident. Chief Customer and Commercial Officer, CX ("CCCO, CX") confirmed that all affected local customers had been notified.

#### *Lay-offs in the Information Technology department*

8. Mr Charles Peter MOK commended the efforts made by CX's technical personnel in handling the incident. He queried whether the incident reflected the negative impact of the company's restructuring, and the downsizing of the Information Technology ("IT") department in recent years. Mr YIU Si-wing, Mr POON Siu-ping, Mr LUK Chung-hung and Dr KWOK Ka-ki made similar remarks. Mr POON Siu-ping enquired about the size of the IT security team. Mr LUK Chung-hung and Mr HO Kai-ming asked whether CX had future plans of more lay-offs. Mr LUK Chung-hung questioned whether lay-off plans might possibly harm aviation safety in the future. CCCO, CX responded that frontline staff, including its IT security team of 12 members, was not affected by the staff

restructuring in 2017 and there was no relation between the restructuring and this incident. The restructuring had been completed and there were no plans for further staff restructuring. CCCO, CX expressed that CX had an on-going plan to expand its local investment and manpower in IT security, and some tasks previously contracted out were being restored in-house. It would also groom local talents to be its IT management trainees.

*Compliance with regulations*

9. Mr CHAN Chun-ying said that listed companies in Hong Kong were obliged to disclose any price-sensitive information ("PSI") to the public, as soon as reasonably practicable after PSI had come to their knowledge. He queried if CX had sought legal advice on whether the company had breached any of the relevant listing conditions for not having disclosed the leakage of customers' personal information in a timely manner, as it might be regarded as PSI. Chairman, CX replied that CX had experience in complying with the disclosure requirements in the Securities and Futures Ordinance (Cap. 571). He said that whether certain information was price sensitive or not was a matter of judgment. According to the guidelines published by the Securities and Futures Commission, issues of considerable public interest, such as the breach of CX passenger data, might not necessarily be materially price sensitive.

10. Ms Claudia MO queried whether CX was prepared to face a potential fine under the European Union's new regulations. Dr CHENG Chung-tai asked for an estimate of the amount of fine CX might be liable to. CEO, CX advised that the company had informed 27 regulatory authorities in 15 jurisdictions about this incident. While CX was prepared to respond to any further enquiries, it was too early to estimate the amount of fine incurred, if any.

11. Mr LAM Cheuk-ting asked whether CX was aware of the Guidance on Data Breach Handling and the Giving of Breach Notifications ("the Guidance") issued by the Office of the PCPD. He queried why CX did not act according to the Guidance. Mr Kenneth LEUNG raised a similar query. Mr AU Nok-hin challenged whether CX had closely followed the Guidance which suggested notifying the authorities in the second step of its four-step handling procedures in the case of data breach. CEO, CX said that the company was aware of PCPD's Guidance. He explained that in this particular incident, the company had tried to provide meaningful and accurate information to affected passengers before proceeding to the subsequent steps according to the guidelines. Attacks being organized in waves and the uncertainty about the intelligibility of the leaked encrypted data added difficulty to the process. CEO, CX said that, with hindsight, the company would have taken a different course of action and would have informed the relevant parties at an earlier opportunity.



12. Mr James TO Kun-sun commented that CX should have exercised its common sense rather than adopting a narrow interpretation of the Guidance. In particular, it should have alerted the public earlier about the data breach, instead of spending time on confirming the details of the lost data for each customer before making the announcement. CEO, CX agreed that with hindsight, the notification should have been advanced.

13. Dr Priscilla LEUNG Mei-fun asked how timely CX had reported the incident to the authorities in comparison with other similar data breaches. PCPD advised that other incident reports were often received within days but there was no specific time limit for reporting data breach incidents in Hong Kong as well as in some other jurisdictions. Mr Alvin YEUNG enquired whether the Guidance could be modified to enhance its deterrent effect. Mr James TO Kun-sun asked PCPD if it was absolutely necessary for a company to gather all the detailed information as specified in the Guidance before it could notify data owners of any security breach leading to the leak of data. PCPD responded that while it was possible to revise the Guidance to give clearer advice on the recommended timing for reporting and disclosing an incident, the interests of all parties should be given due consideration. PCPD indicated that the issues as raised by members would be considered in the review.

*(Post-meeting note: PCPD issued a set of revised Guidance in January 2019.)*

14. Mr AU Nok-hin enquired whether the duration of CX's retention of personal data complied with the relevant regulations. CCCO, CX responded that CX handled personal data according to its internal guidelines and would be willing to improve upon the regulators' advice as appropriate.

#### *Enforcement actions*

15. Mr LAU Kwok-fan questioned why PCPD did not carry out a compliance investigation upfront but had, instead, conducted a compliance check first. PCPD explained that it had been an established practice that a compliance check should precede a compliance investigation. The objective was to minimize the damages caused by a data breach to the affected persons as early as possible and to examine whether there existed reasonable grounds to believe that there might be a contravention of the Personal Data (Privacy) Ordinance. (Cap. 486). In fact, many of the recent incidents involved security issues where compliance checks were necessary to gather the relevant information.

16. Mr Kenneth LEUNG queried whether CX had complied with the Guidance issued by PCPD and whether there were legal sanctions if a person failed to observe the Guidance. PCPD advised that as the subject investigation was still in progress, no details in response to Mr LEUNG's query could be released at this stage. However, in general, a person might be served an enforcement notice if he or she was found to have contravened the data protection principles under Cap. 486. The matter might also be referred to the Police for criminal investigation and to the Secretary for Justice for prosecution. PCPD added that contravention of the requirements in an enforcement notice was liable to a fine of up to HK\$50,000 and two years' imprisonment.

*Regulations and penalty of greater deterrence*

17. With reference to EU's General Data Protection Regulation ("GDPR"), Mr LAU Kwok-fan queried whether the Administration would review the relevant provisions in Cap. 486 to introduce requirements for incidents of data breaches to be disclosed, say, within 72 hours. Dr CHENG Chung-tai, Mr Jeffrey LAM Kin-fung and Mr AU Nok-hin made similar comments. Mr POON Siu-ping and Dr KWOK Ka-ki asked for a timetable of the review. Mr Kenneth LEUNG and Mr Alvin YEUNG said that the current regulatory regime lacked deterrent effect. Mr Alvin YEUNG and Ms Alice MAK Mei-kuen commented that the level of penalty should be increased.

18. PCPD advised that under the current law there is no mandatory requirement for any organization to file a notification in cases of data leakage. PCPD said that his office had started reviewing Cap. 486 taking into consideration the provisions in GDPR. Mandatory requirements for notification, prosecution process as well as the penalty levels were among the areas to be reviewed. He added that all suggestions for amendment should be considered in the light of the interest of all stakeholders; and a review report would be submitted to Constitutional and Mainland Affairs Bureau for follow-up as soon as possible. SCMA agreed that there was room for amending Cap. 486 and the Administration would take the results of the compliance investigation into consideration while keeping an open mind about the amendment proposals.

19. Dr Elizabeth QUAT said that Cap. 486 should be updated to enhance protection of personal privacy. She said that there had been considerable progress in the application of information technology since PCPD's last review of Cap. 486, and European Union's GDPR had been introduced in 2018. Cyber security laws had been instituted in many overseas jurisdictions to safeguard personal data and to prescribe rules on how incidents of personal data breaches should be reported. Dr QUAT suggested that similar legislation should be made

in Hong Kong so that the statutory framework for protection of privacy would keep pace with development.

20. Dr Elizabeth QUAT further suggested that the Administration should make reference to international standards such as ISO27001 and introduce legislation that would regulate how an organization protect and manage clients' personal data. Such legislation should prescribe, for example, the purpose of collecting personal data, how the data would be used, how and for how long the data were to be stored, and the mechanism of how a breach of data security should be reported. Dr QUAT suggested that a separate meeting should be held to discuss with the Administration on the legislation matters, and that public hearing sessions should be held to collect stakeholders and public views.

*Precautionary actions to be taken by affected customers*

21. Ms Alice MAK Mei-kuen commented that CX gave unclear instructions on registering the identity ("ID") monitoring service in its email to the affected passengers and she demanded improvement in customer service. CEO, CX responded that it had prepared quick reference notes to help people understand the free ID monitoring service it had provided as a remedial measure. In response to the enquiry from Mr Tony TSE Wai-chuen, PCPD advised that if members of the public found any abnormalities with their personal accounts of the airline concerned or credit card accounts, they should contact the airline and the related financial institutions. They should also change the account passwords and enable two-factor authentication to protect their personal data.

*Accountability of the management board*

22. Ms Claudia MO and Dr CHENG Chung-tai enquired whether the CX management board would step down to apportion accountability and whether the extra costs associated with the aftermath of this incident would affect the employment of frontline staff. Chairman, CX said the current mechanism where directors and broad members were elected by shareholders should ensure that the management board was properly accountable. He added that frontline staff would not need to worry about their jobs due to this incident.

*Compensation to affected customers*

23. Mr CHAN Hak-kan, Mr CHAN Chun-ying, Ms Alice MAK Mei-kuen, Mr POON Siu-ping and Mrs Regina IP LAU Suk-yee questioned whether CX had any plans to compensate the affected passengers. Mr CHAN Chi-chuen asked whether CX would compensate for affected customers who might not have sustained economic damages. Mr Michael TIEN Puk-sun further

suggested that CX should take active steps rather than wait for affected customers to claim compensation, and that the company should scale the compensation according to the damage suffered. He also suggested that CX should extend the free ID monitoring service to three years and promote the free ID monitoring service by contacting each affected customer, and that the company should boost the registration rate of the service by offering them financial incentives. CEO, CX said that affected passengers had already been informed individually about the details pertaining to the leakage of their personal data and how they might make use of the provided ID monitoring service to prevent further damage. He added that passengers were invited to seek assistance from CX in case their personal data were found to have been used improperly. Chairman, CX added that CX would introduce measures to recover the goodwill of Hong Kong people. Dr Priscilla LEUNG Mei-fun enquired whether the Administration could facilitate the process of claiming compensation by such a large number of victims. SCMA advised that customers might approach the Consumer Council for assistance under the prevailing practice.

24. Mr Paul TSE Wai-chun commented that CX was itself a victim of the computer security attack. As its database was probably interconnected with other interfaces on the Internet, CX might not be entirely responsible for the data leakage. It might thus be inappropriate to demand compensation from CX unless the damage was proved to be caused by the company.

#### *Goodwill and customers' confidence*

25. Mr CHAN Chun-ying enquired whether CX would implement measures such as two-factor authentication log-in process to enhance cyber security. Mr Jeffrey LAM Kin-fung and Mrs Regina IP LAU Suk-ye asked what measures CX would adopt to restore the company's image and customers' confidence in the company. CCCO, CX replied that by constantly improving its fleet, network of destinations and passenger experience, the company was confident that its image could be restored. It also had plans to launch promotion programmes as a gesture to show gratitude for customers' continuous support.

*(Post-meeting note: The Chairman extended the scheduled meeting duration for 15 minutes to allow more thorough discussion.)*

#### Motions

26. Mr CHAN Chi-chuen, Mr Michael TIEN Puk-sun and Dr Elizabeth QUAT respectively proposed a motion under the agenda item. The Chairman ruled that these motions were related to the item under discussion. Given that

there was insufficient time, the Chairman directed, after consulting the Panels, that these motions should only be handled after all members were given the chance to contribute to the discussion.

*(Post-meeting note: These motions were not put to vote due to time constraints.)*

*First motion proposed by Mr CHAN Chi-chuen:*

本事務委員會聯席要求因資訊系統管理不善而令 900 萬客戶資料被盜用的國泰航空必須採取措施，確保客戶資料不再被盜用，日後若發現客戶資料被盜用必須立即公布，並就今次多名客戶資料被盜用的事件立即作出實際行動以賠償資料被盜的客戶的損失。

(Translation)

These Panels jointly request that Cathay Pacific Airways, whose poor information technology system management has led to the personal data of its nine million clients being stolen, must take measures to ensure no reoccurrence of the theft of clients' data, make immediate announcement upon discovery of any theft of clients' data in the future, and take specific actions immediately in respect of this massive theft of clients' data by compensating clients for the losses arising from the data theft.

*Second motion proposed by Mr Michael TIEN Puk-sun:*

本委員會要求政府當局督促國泰採取下列補救措施：

1. 按嚴重程度賠償受影響乘客
2. 主動逐一聯絡受影響乘客
3. 採取任何可行方法提升身份監察服務登記率，例如如果身份監察服務發現任何問題，再按嚴重程度賠償
4. 延長免費身份監察服務至三年或以上。

(Translation)

This Committee requests the Administration to urge Cathay Pacific to take the following remedial measures:

1. to compensate clients affected by the incident according to the severity of their losses;
2. to take the initiative to contact the affected clients one by one;

3. to try every possible means to increase the rate of enrolment in IdentityWorks, an identity monitoring service, such as compensating clients according to the severity of their losses upon detection of any problems by the identity monitoring service; and
4. to extend the free identity monitoring service to three years or more.

*Third motion proposed by Dr Elizabeth QUAT:*

國泰航空自今年 3 月已發現公司資訊系統受到黑客攻擊，並於 5 月已確認超過 940 萬名客戶的資料被不當取覽，事態極其嚴重，本應立即開誠布公地公開情況，讓受影響客戶及早進行各項補救措施，然而，令人憤怒的是，國泰拖延足足七個月，才公布整件事件，完全無視市民的知情權；此外，事件亦反映現行保障個人私隱資料的法例急需檢討，就此，本會促請政府應檢討《個人資料(私隱)條例》，並同時研究制訂網絡安全法，以提升本港網絡安全水平。

(Translation)

Cathay Pacific Airways discovered that its information technology systems were attacked by hackers as early as in March this year and confirmed that personal data of over 9.4 million clients were affected by the unauthorized access in May. In view of the extreme seriousness of the incident, Cathay Pacific should have immediately made public the incident in an open and transparent manner to enable the affected clients to take various remedial measures as soon as possible. However, it is outrageous that Cathay Pacific did not disclose the entire incident until seven months later, in total disregard of the public's right to know. Besides, this incident also reflects an urgent need to review the existing legislation on the protection of personal data privacy. In this connection, this Committee urges the Government to review the Personal Data (Privacy) Ordinance and also study the enactment of cyber security law, so as to enhance the cyber security in Hong Kong.

Follow-up actions

27. CX was requested to provide members with its written response to Mr Charles Peter MOK's questions about incident log, policy on third-party service providers, resources allocation in IT security, etc.

*(Post-meeting note: CX's written response was circulated to members as LC Paper No. CB(4)242/18-19(01) by e-mail on 22 November 2018.)*

**III. Any other business**

28. There being no other business, the meeting ended at 10:46 am.

Council Business Division 1  
Legislative Council Secretariat  
27 August 2019