CATHAY PACIFIC

LC Paper No. CB(2)230/18-19(01)

Response to questions in letter dated 5 November 2018 by
Cathay Pacific Airways Limited
for the
Joint Meeting on Wednesday, 14 November, 2018
of the
Panel on Constitutional Affairs
Panel on Information Technology and Broadcasting
Panel on Security

The Legislative Council ("**LegCo**") has requested Cathay Pacific Airways Limited ("**Cathay**") to attend a joint meeting of the Panel of Constitutional Affairs, Panel on Information Technology and Broadcasting and the Panel on Security on Wednesday, 14 November, 2018. LegCo has also requested a written response to questions prepared by the Hon. Charles Mok to be provided on or before noon, 12 November 2018. Our written response to the questions prepared by the Hon. Charles Mok is set out below.

1. **How did you know your systems had suspicious activities in March? How did the monitoring system pick up the suspicious activity/attack? The time suspicious activity surfaced and was the system continuously attacked after the detection? If so, how long was the system continuously being attacked? In May how did you confirm the details of passenger details accessed?**

Cathay became aware of suspicious activity on its network related to the attack in March 2018. Initially, the only evidence of known suspicious activity pertained to a brute force attack on user accounts. At this stage, an initial evaluation commenced and following this analysis, a thorough investigation launched with the assistance of a leading cybersecurity firm. Cathay immediately took action to contain the Incident based on known activities at that time and commenced an internal investigation. Cathay was subject to further attacks which were at their most intense in March, April and May but continued thereafter. By early May, evidence of unauthorised access and/or exfiltration of data by the attackers was confirmed based on forensic evidence. This was the first phase of the Incident.

During the second phase, work on the details of the accessed data continued. The two big issues were: which passenger data had been accessed or exfiltrated and, since the affected databases were only partially accessed, whether the data in question could be reconstructed outside Cathay's IT systems in a readable format useable to the attacker(s). Conclusions on these issues proved difficult and time-consuming and were only reached in mid-August.

During the third phase, the emphasis shifted to identifying the compromised data types for each affected passenger. Cathay wanted to be able to give a single, accurate and meaningful notification to each affected passenger, rather than to provide an overly broad and non-specific notice. It was not until 24 October that Cathay had completed the identification of the personal data that pertained to each individual passenger.

2. **Earlier, you sent a personalised email to each affected passenger which details the particular data types that were accessed. Can CX confirm that no other data types were accessed for each affected passenger other than those listed in the email?**

   We have identified all the personal data types that were accessed for each affected passenger to whom we have sent an email. The emails sent out to each affected passenger should therefore contain details of all personal data types accessed for that particular passenger.

3. **Do all CX databases contain the log review function? (Especially in relation to the affected databases/systems in this incident).**

   All Cathay databases and database servers have logging capabilities enabled at the OS and database level.

4. **If your system has the function mentioned in 3, did you use that function to investigate the details, contents and that time that the particular piece of data was collected and accessed by the hackers?**

   Cathay used all available logging to assist in the investigation, which consisted of manual log review and live response analysis. Log review and analysis were critical to the investigation and determining the activities of the attacker.

5. **Have you found any malware, Trojan and payload in the databases that were accessed. If so, what are the characteristics of these bad software**

   Certain malware and utilities used by the attackers have been discovered. The malware and utilities vary in capabilities, such as giving the attacker the ability to conduct reconnaissance and move within the environment. The signatures were not previously known, and therefore were not detected by Cathay's up to date anti-virus system.

6. **Do you have a policy that restrict third party suppliers in the access or connection to your database? If so, what are the details?**

   Cathay has a policy in place that restricts third-party connections and access to the Cathay network.

7. **Do you have a consistent and constant detection and monitoring mechanism to threats posed by APTs?**

   Cathay has had in place monitoring and detection mechanisms. Since March 2018, Cathay has also implemented an advanced endpoint detection and response system.

8. **Do you have any remedial measures to prevent similar events from happening? If so, please elaborate.**

Remediation steps were taken from the beginning of our investigation and continue through today. Some of these steps were short term to protect our perimeter and keep the attackers out. Some were longer term and more strategic. We blocked IPs, shut down certain servers, made changes to our protections such as firewalls and set up alerting of certain activity. We launched an advanced threat detection system across the environment. As the investigation progressed, we began implementing more strategic actions such as extending network segmentation and further security improvements. Strategic and long term remediation efforts have also been developed and will be implemented. It should be noted that we did have a robust security program and security defences in place. However, this was a very sophisticated attack and used malware not seen or know before.

Cathay Pacific Airways Limited
November 2018