Summary of Key Events: 4

- 1 Week later, on 4 July 2018, an IHiS administrator for the SCM system noticed suspicious queries being made on the SCM database.

- Working with other IT administrators, ongoing suspicious queries were terminated, and measures were put in place to prevent further queries to the SCM database.

- These measures proved to be successful, and the attacker could not make any further successful queries to the database after 4 July 2018.

Summary of Key Events: 5

- Between 11/6 & 9/7/18, the persons who knew of & responded to the incident were limited to IHiS' line-staff & middle management from various IT administration teams, & the security team.

- After 1 month, on 9/7/18, IHiS senior management were finally informed of the Cyberattack…

- 3 days later, 10/7/18, matter was escalated to Cyber Security Agency ("CSA"), SingHealth's senior management, the Ministry of Health ("MOH"), and the Ministry of Health Holdings ("MOHH")

Summary of Key Events: 6(*)

- Starting from 10 July 2018, IHiS and CSA carried out joint investigations and remediation.

- Several measures aimed at containing the
  - existing threat,
  - eliminating the attacker's footholds, and
  - preventing recurrence of the attack were implemented.

- In view of further malicious activities on 19 July 2018, internet surfing separation was implemented for SingHealth on 20 July 2018.

- No further suspicious activity was detected after 20 July 2018.

Summary of Key Events: 7

- The public announcement was made on 20 July 2018, and patient outreach and communications commenced immediately thereafter.

- SMS messages were used as the primary mode of communication, in view of the need for quick dissemination of information on a large scale.

- **COI Committee has identified 5 key Findings!**

KEY FINDING 1

- **IHiS staff did not have adequate levels of cybersecurity awareness, training, and resources**
  - **to appreciate the security implications of their findings and**
  - **to respond effectively to the attack.**