Summary of Key Events: 1

- The attacker gained initial access to SingHealth's IT network around 23/8/17, infecting front-end workstations, most likely through ***phishing attacks***.
- Attacker then lay dormant for 4 months, before commencing lateral movement (6 months) in the network between Dec2017 and Jun2018, compromising many endpoints and servers, including the Citrix servers located in SGH, which were connected to the SCM database.
- Along the way, the attacker also compromised a large number of user and administrator accounts.

Summary of Key Events: 2

- Starting from May 2018, the attacker made use of compromised user workstations in the SingHealth IT network and suspected virtual machines to remotely connect to the SGH Citrix servers.

Summary of Key Events: 3

- IHiS' IT administrators first noticed unauthorised logins to Citrix servers & failed attempts at accessing the SCM DB on 11 June 2018.

- On 27 June 2018, the attacker began querying the SCM database, stealing and exfiltrating patient records, and

- doing so undetected by IHiS.

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.**