Singhealth Data Breach

(directly based on COI report)

Overview Diagram slide 5

Crisis in a Nutshell

- Between 23/8/17 -20/7/18, a cyberattack of unprecedented scale & sophistication was carried out on Singhealth patient database.
- DB was illegally accessed & personal particulars of 1.5 million patients, including names, NRIC numbers, addresses & dates of birth, were exfiltrated over the period of 27/6/18 to 4/7/18.
- Around 159,000 of these 1.5 million patients also had their outpatient dispensed medication records exfiltrated.
- The Prime Minister's personal and outpatient medication data was specifically targeted and repeatedly accessed.

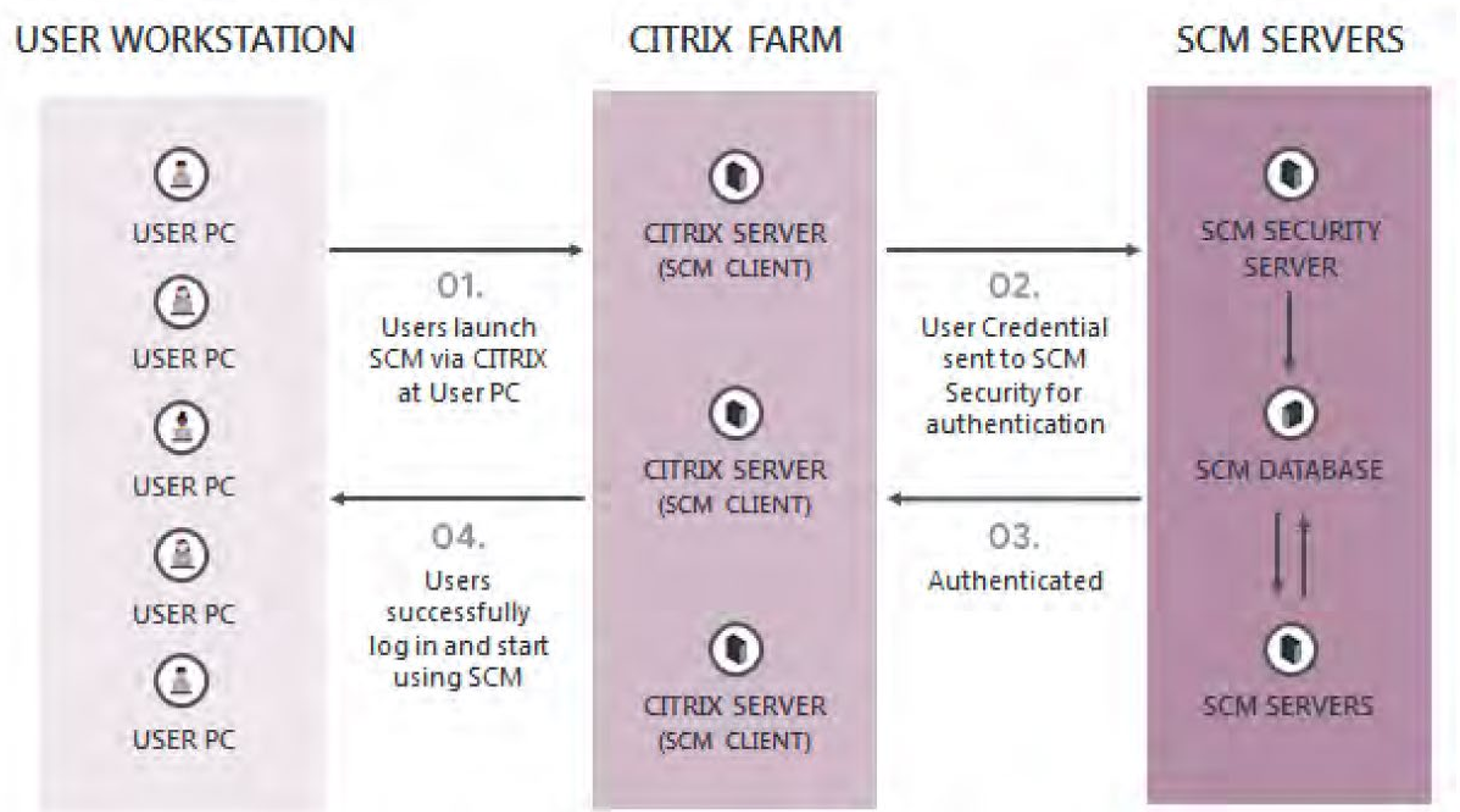
Crisis in a Nutshell

- The crown jewels of the SingHealth network are the patient electronic medical records contained in the SingHealth "SCM" database.
- The SCM is an electronic medical records software solution, which allows healthcare staff to access real-time patient data.
- It can be seen as comprising front-end workstations, Citrix servers, and the SCM database.
- Users would access the SCM database via Citrix servers, which operate as an intermediary between front-end workstations & the SCM database.
- The Citrix servers played a critical role in the Cyber Attack.

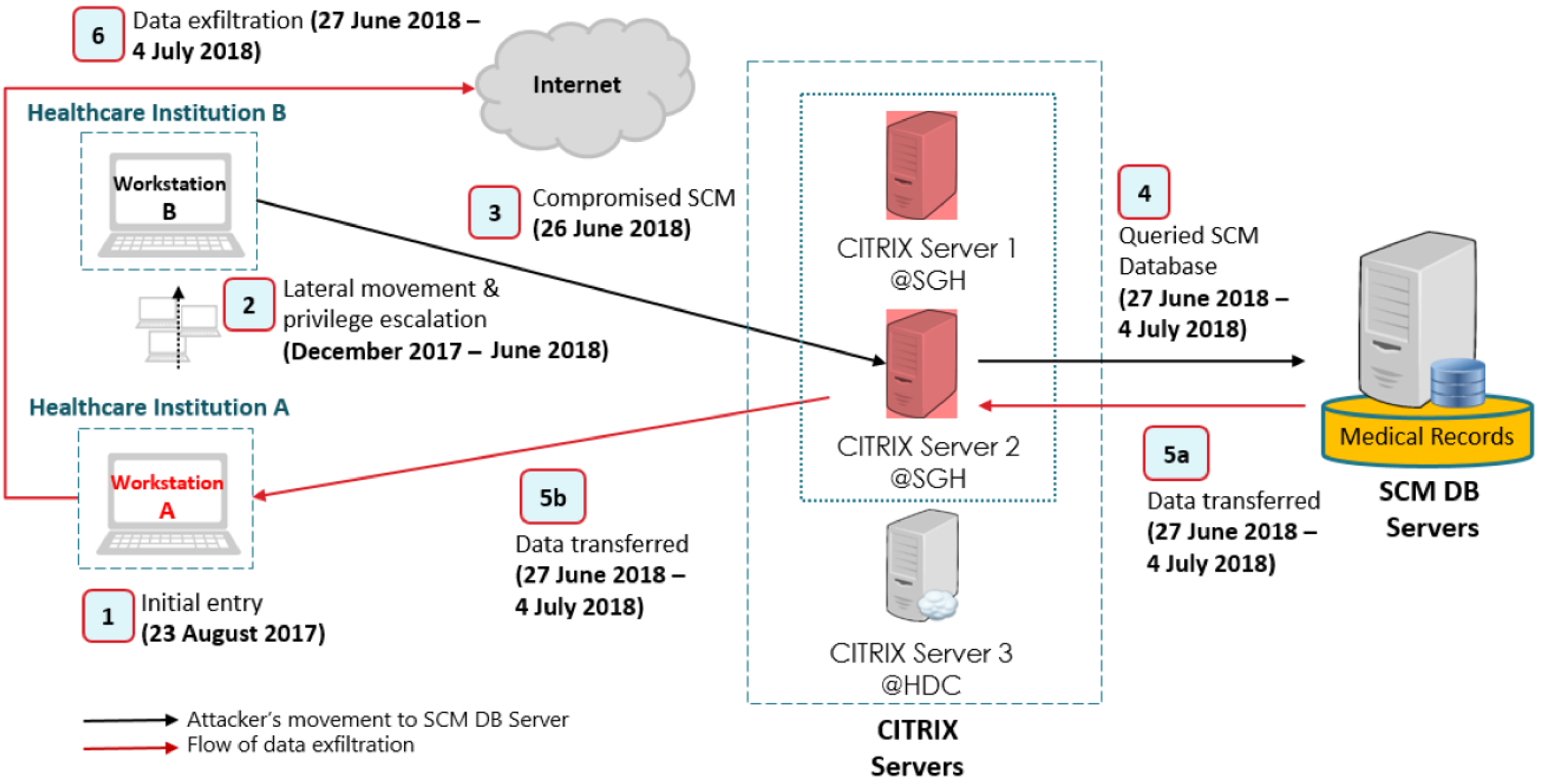
Crisis in a Nutshell

- At time of the Cyber Attack, SingHealth owns the SCM system.
- Integrated Health Information Systems Private Limited (“IHiS”) was responsible for administering and operating the system, including implementing cybersecurity measures.
- IHiS was also responsible for security incident response and reporting.

Figure 3:SingHealth user authentication process to access the SCM Database


USER WORKSTATION
CITRIX FARM
SCM SERVERS
USER PC
USER PC
USER PC
USER PC
USER PC
01.
Users launch SCM via CITRIX at User PC
04.
Users successfully log in and start using SCM
CITRIX SERVER (SCM CLIENT)
CITRIX SERVER (SCM CLIENT)
CITRIX SERVER (SCM CLIENT)
02.
User Credential sent to SCM Security for authentication
03.
Authenticated
SCM SECURITY SERVER
SCM DATABASE
SCM SERVERS

Key Events of the Cyberattack -workflow



6 Data exfiltration **(27 June 2018 – 4 July 2018)**

3 Compromised SCM **(26 June 2018)**

2 Lateral movement & privilege escalation **(December 2017 – June 2018)**

4 Queried SCM Database **(27 June 2018 – 4 July 2018)**

5a Data transferred **(27 June 2018 – 4 July 2018)**

5b Data transferred **(27 June 2018 – 4 July 2018)**

1 Initial entry **(23 August 2017)**

Attacker's movement to SCM DB Server

Flow of data exfiltration

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.