Observations on the overall management of SGH Citrix servers

They were treated as not mission critical, unlike SCM database

- The SGH Citrix servers were not monitored for real-time analysis and alerts of vulnerabilities and issues arising from these servers.
- Vulnerability scanning, which was carried out for mission-critical systems, was not carried out for the SGH Citrix servers.
  - Vulnerability scanning is an inspection of the potential points of exploit on a computer to identify gaps in security.

Internet connectivity in the SingHealth IT network increased the attack surface

- The SingHealth network's connection to the Internet, while serving their operational needs, created an avenue of entry and exit for the attacker.
- This allowed the attacker to make use of an internet-connected workstation (Workstation A) to gain entry to the network, before making his way to the SCM database to steal the medical data.

Internet connectivity in the SingHealth IT network increased the attack surface

- The security risks arising from internet-connectivity in the SingHealth network were raised by CSA to MOH from as early as August 2015;
- By June 2017, the healthcare sector had determined, that
  - internet access would be removed for staff that did not require the internet for work,
  - for staff that required the internet for work, access would be through a secure internet access platform which, at that time, was to take the form of a 'remote browser'.

Versions of Outlook used by IHiS were not patched against a publicly available hacking tool

- The attacker was able to install the hacking tool (publicly available) on Workstation A on 1 December 2017 by exploiting a vulnerability in the version of the Outlook application installed on the workstation!

- A patch that was effective in preventing the vulnerability from being exploited (and thus to prevent the installation of the tool) was available since late-2017!

- Clear need to improve software upgrade policies!

Extensive C2 Infrastructure

CSA's forensic analysis revealed a number of network Indicators of Compromise ("**IOCs**") which appeared to be overseas C2 servers. CSA has explained that generally, the C2 servers were used for:

- Infection: where the server is used as a means of dropping malware into the system it is trying to infect;
- Data exfiltration: there were indications of technical data being sent to the servers; and
- Beacon: infected machines may have connected to C2 servers to establish a 'heartbeat', which refers to a slow, rhythmic communication meant just to sustain communications.