In Singapore’s worst ever cyberattack, dated 2018, hackers infiltrated the databases of SingHealth, the largest group of healthcare institutions within the island. The personal particulars of 1.5 million patients, including the outpatient prescriptions of Prime Minister Lee Hsien Loong and a few ministers, were stolen.

About 1.5 million patients who visited SingHealth's specialist outpatient clinics and polyclinics from May 1, 2015, to July 4, 2018, had their personal particulars illegally accessed and copied. The records were not tampered with.

Initial investigations showed that one SingHealth front-end workstation was infected with malware through which the hackers gained access to the database. The data theft happened between June 27 and July 4.More malicious activities were observed during heightened monitoring. But no more data had been stolen. Healthcare services were not disrupted and patient care was not compromised during the attack, said the authorities.

Integrated Health Information Systems (IHiS), an equivalent of a safety patrol, detected unusual activity in one of SingHealth's IT databases. Immediate security measures are taken, including:

• Changing servers and database administration passwords

• Restricting domain administration access

• Monitoring database and system logs

• Blocking connections to prevent further access

It was probably a code injection into a work terminal that would have access to the mainframe through which data packets are sent to and fro, and the intruders took advantage of the fact by attacking from the client to the server through this established connectivity from client to server. This enabled them to hijack the large amount of individuals data and get away with it. Personal particulars that would reveal sensitive information, such as physical addresses, health conditions, and such would be compromising the purportedly sensitive information that should have been secured in a safe location.

The countermeasures taken are akin to that of what government agencies take when they embark on the counteroffensive.

SingHealth has imposed a temporary Internet surfing separation on all of its 28,000 staff’s work computers. The Cyber Security Agency (CSA) will work closely with all key sectors of the Government to enhance their critical information infrastructure systems immediately. The sectors are energy, water, banking and finance, healthcare, transport (which includes land, maritime and aviation), info communications, media, security and emergency services, and the Government. The authorities will also not introduce any new information and communications technology systems while they review existing cyber-security measures and implement any additional security safeguards.

As well, Minister-in-charge of Cyber Security S. Iswaran will convene a Committee of Inquiry (COI) to investigate the cyber-attack and recommend measures to strengthen public-sector IT systems against similar attacks. The COI will be chaired by Mr Richard Magnus, a retired senior district judge and member of the Public Service Commission.

All these would accumulate to form a more comprehensive review policy which would allow more stakeholders to come together to formulate a better response system if possible to mitigate such intrusions in the future, especially so with the occurred security breach.

Amongst some of the recommendations would be that of :

1. An enhanced security structure and readiness must be adopted by IHiS and Public Health Institutions

Cybersecurity must be viewed as a risk management issue, and not merely a technical issue. Decisions should be deliberated at the appropriate management level, to balance the trade-offs between security, operational requirements, and cost.

IHiS must adopt a “defence-in-depth” approach.

 Gaps between policy and practice must be addressed.

1. The cyber stack must be reviewed to assess if it is adequate to defend and respond to advanced threats

 Identify gaps in the cyber stack by mapping layers of the IT stack against existing security technologies.

 Gaps in response technologies must be filled by acquiring endpoint and network forensics capabilities.

The effectiveness of current endpoint security measures must be reviewed to fill the gaps exploited by the attacker.

Network security must be enhanced to disrupt the ‘Command and Control’ and ‘Actions on Objective’ phases of the Cyber Kill Chain.

Application security for email must be heightened.

1. Staff awareness on cybersecurity must be improved, to enhance capacity to prevent, detect, and respond to security incidents

The level of cyber hygiene among users must continue to be improved.

A Security Awareness Programme should be implemented to reduce organisational risk.

IT staff must be equipped with sufficient knowledge to recognise the

signs of a security incident in a real-world context.

This would help to keep ourselves on the offensive with regards to approaching the issue at hand on cybersecurity and defending on the threats.