Knowing the unknown

Today Agenda:

i. **Sharing of Recent Public Breaches**
ii. **Root Causes Behind the Public Breaches**
iii. **Measures to Implement to Reduce Cybersecurity Risk Exposure**
iv. **What does this mean to 3rd line of defense**

Kok Tin Gan
Cybersecurity Partner
PwC Hong Kong
kok.t.gan@hk.pwc.com
+852 9728 0211

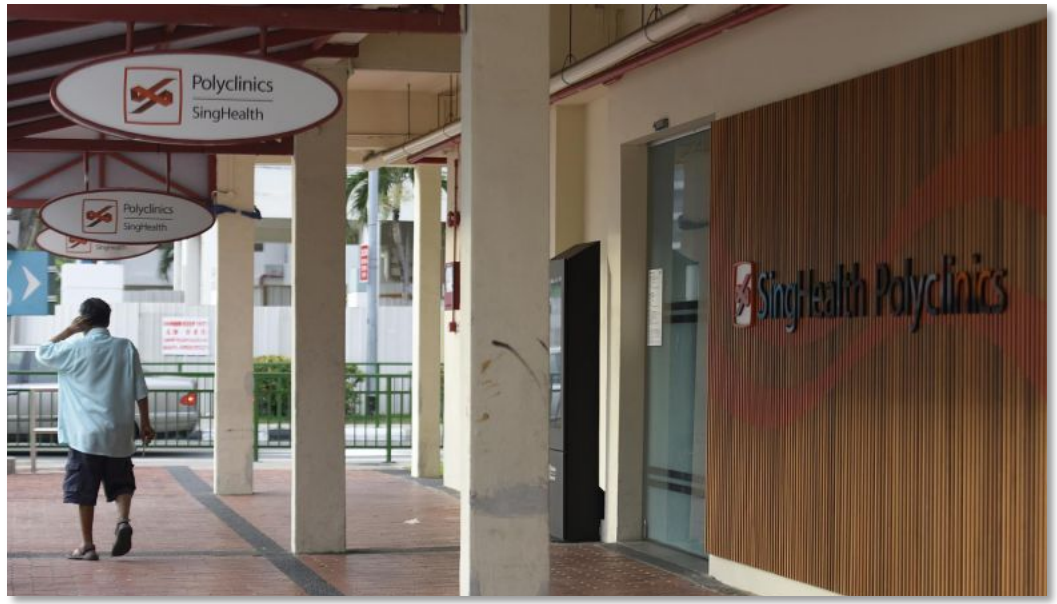
Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

SINGAPORE - The cyber attack in Singapore that led to the leak of 1.5 million SingHealth patients' personal data was the work of an "advanced persistent threat" group typically linked to foreign governments, Parliament heard on Monday (Aug 6).

Mr Tan, the only witness to testify during Tuesday's public hearing, was alerted to suspicious network activities as early as mid-June, when they were first spotted by his subordinates. "**I did not read any of these e-mails at the time they were sent, as I was on overseas leave in Japan** from June 9 to 17. I only read them when I returned to Singapore on Monday, June 18," he said.

Advanced persistent threats (APTs) are stealthy and continuous computer hacking processes to gain intelligence or steal information.

"This refers to a class of **sophisticated cyber attackers**, typically state-linked, who conduct extended, carefully planned cyber campaigns, to steal information or disrupt operations," said Minister for Communications and Information S. Iswaran in response to a record 19 questions filed by MPs, the highest in this term of Parliament on a single issue.



Improve staff awareness of cybersecurity, **better incident response** proposed as SingHealth COI ends. This, Mr Kwek added, can be done by having staff training that expresses the idea that cybersecurity is everyone's job and not just the IT department's. Training should also be ongoing and employees be tested on their awareness through things like mock phishing exercises in a formalised programme, rather than in an ad hoc manner, he said.

Cyber Attack Kill Chain

IT administrators **could not fully appreciate the security** implications of their findings, and were unable to co-relate these findings with the tactics, techniques, and procedures of an **advanced cyber attacker**.

The SGH Citrix servers were not adequately secured against unauthorised access. Notably, the process **requiring 2-factor authentication ("2FA") for administrator access** was not enforced as the exclusive means of logging in as an administrator. This allowed the attacker to access the server through other routes that did not require 2FA.

These included **weak administrator account passwords** and the need to improve **network segregation** for administrative access to critical servers such as the domain controller and the Citrix servers.

The Cluster ISO did not understand the significance of the information provided to him, and did not take any steps to better understand the information**. Instead, he effectively abdicated to the SIRM the responsibility of deciding whether to escalate the incident.**

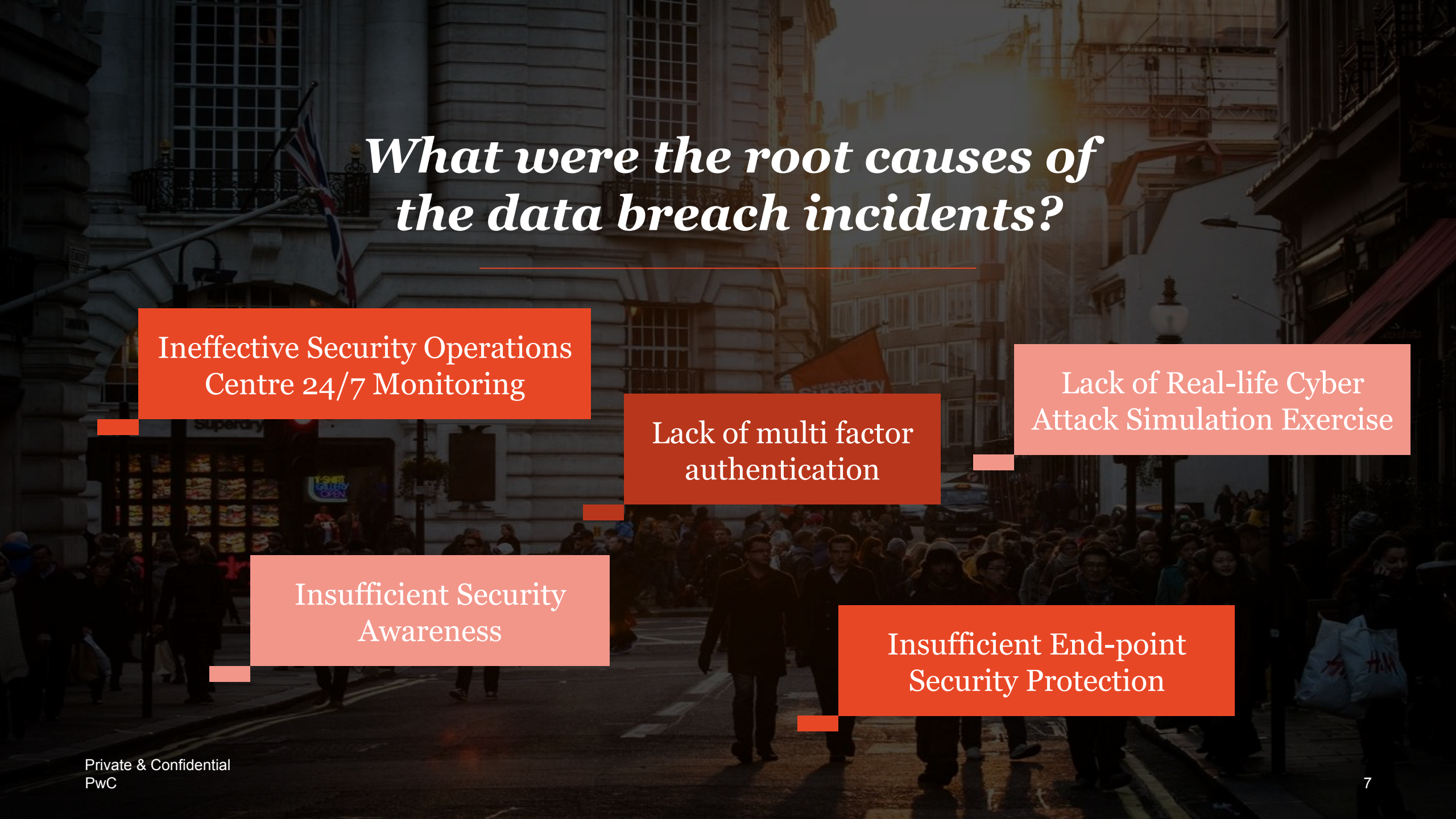
There was a **coding vulnerability in the SCM application** which was likely exploited by the attacker to obtain credentials for accessing the SCM database

The attacker was stealthy but not silent, and signs of the attack were observed by IHiS' staff. Had IHiS' staff been able to recognise that an attack was ongoing and take appropriate action, the attacker could have been stopped before it achieved its objectives.

There **were no existing controls to detect bulk queries being made to the SCM database**. While bulk queries are not uncommon as they are used for generating reports, the queries run by the attacker were anomalous in a number of ways

There was no explicit mention of the **need to change the *local administrator* account passwords** to meet the new requirement, explaining that it did not occur to them at the time the management response was being discussed.

The failure to block the suspicious IP address across the whole network and to investigate Workstation A constituted a significant missed opportunity to prevent the attack.



What were the root causes of the data breach incidents?

Ineffective Security Operations Centre 24/7 Monitoring

Lack of multi factor authentication

Lack of Real-life Cyber Attack Simulation Exercise

Insufficient Security Awareness

Insufficient End-point Security Protection

What are the measures to implement to reduce the cybersecurity risk exposure?

Security Awareness

Establish 24/7 SOC Monitoring Capability

Red Teaming Exercise

Two Factor Authentication

Endpoint Security

Network Segmentation

What does this mean to 3rd line of defense?

Independent comfort

Partnership

Controls vs Defense

Skillsets

Effectiveness

Demonstration

Thank you for listening

Kok Tin Gan
Cybersecurity Partner
PwC Hong Kong
kok.t.gan@hk.pwc.com
+852 9728 0211