# T7 Security Management Practices

Group 4:

Darren Ong
Lee Chun Yuen
Lim Jun Kuang, Lionel

# Part 1 Question 1

Consider this performance measure: Percentage of vulnerabilities remediated within organization -specified time frames, it is a/an _____ measure.

a. Implementation
b. Effectiveness/efficiency
c. Impact
d. All of the above

# Part 1 Question 1

Consider this performance measure: Percentage of vulnerabilities remediated within organization -specified time frames, it is a/an _____ measure.

a. Implementation
b. **Effectiveness/efficiency**
c. Impact
d. All of the above

# NIST 800-55r1 Appendix Section Page A-3

**Measure 2: Vulnerability Management (program-level)**

| Field | Data |
|---|---|
| Measure ID | Vulnerability Measure 1 |
| Goal | • *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products.<br>• *Information Security Goal:* Ensure all vulnerabilities are identified and mitigated. |
| Measure | Percentage (%) of high[13] vulnerabilities mitigated within organizationally defined time periods after discovery<br>NIST SP 800-53 Controls: RA-5; Vulnerability Scanning |
| Measure Type | Effectiveness/Efficiency |

# Part 1 Question 2

Consider this performance measure: Percentage of individuals screened before being granted access to organizational information and information systems, it is a/an _____ measure.

a. Implementation
b. Effectiveness/efficiency
c. Impact
d. All of the above

# Part 1 Question 2

Consider this performance measure: Percentage of individuals screened before being granted access to organizational information and information systems, it is a/an_____ measure.

a. Implementation
b. Effectiveness/efficiency
c. Impact
d. All of the above

# NIST 800-55r1 Appendix Section Page A-18

**Measure 15: Personnel Security (PS) (program-level and system-level)**

| Field | Data |
|---|---|
| Measure ID | Personnel Security Screening Measure 1 (or a unique identifier to be filled out by the organization) |
| Goal | • *Strategic Goal:* Ensure an environment of comprehensive security and accountability for personnel, facilities, and products.<br>• *Information Security Goal:* Ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions. |
| Measure | Percentage (%) of individuals screened before being granted access to organizational information and information systems<br>NIST SP 800-53 Controls – AC-2: Account Management and PS-3: Personnel Screening |
| Measure Type | Implementation |

# Part 1 Question 3

What act has Mr Ler been charged under? (Please select all the options that apply)

a. PDPA
b. Computer Misuse Act
c. Official Secrets Act
d. Penal Code

# Part 1 Question 3

What act has Mr Ler been charged under? (Please select all the options that apply)

a. PDPA
b. Computer Misuse Act
c. Official Secrets Act
d. Penal Code

# Grounds of Decision for Interim Orders Committee

5. The current status of each of the aforesaid criminal proceedings are as follows:-

5.1. Penal Code Charges: On 17 September 2018, Dr Ler was convicted in the State Courts of all four Penal Code Charges. He was sentenced on 27 September 2018 to a global sentence of 24 months' imprisonment. Dr Ler has appealed against his conviction and sentence for the Penal Code Charges and such appeal is scheduled to be heard by the High Court in March 2019. Pending the hearing of such appeal, the sentence of imprisonment has been stayed and Dr Ler is on bail.

5.2. OSA Charge: Dr Ler was charged with the OSA Charge on 24 June 2016. The OSA Charge is presently pending further action by the Attorney-General's Chambers.

5.3. Drug Charges: On 3 March 2018 and 27 September 2018, Dr Ler was charged in the State Courts for the Drug Charges. The trial of the Drug Charges is scheduled to be heard in the State Courts from 29 May 2019.

# Part 2

Singapore HIV Data Breach

# What data has been compromised?

Details of all **14,200 people** diagnosed with HIV here since 1985 - till 2013 for locals (**5,400**) and 2011 for foreigners (**8,800**), with details of **2,400 people** who were their contacts.

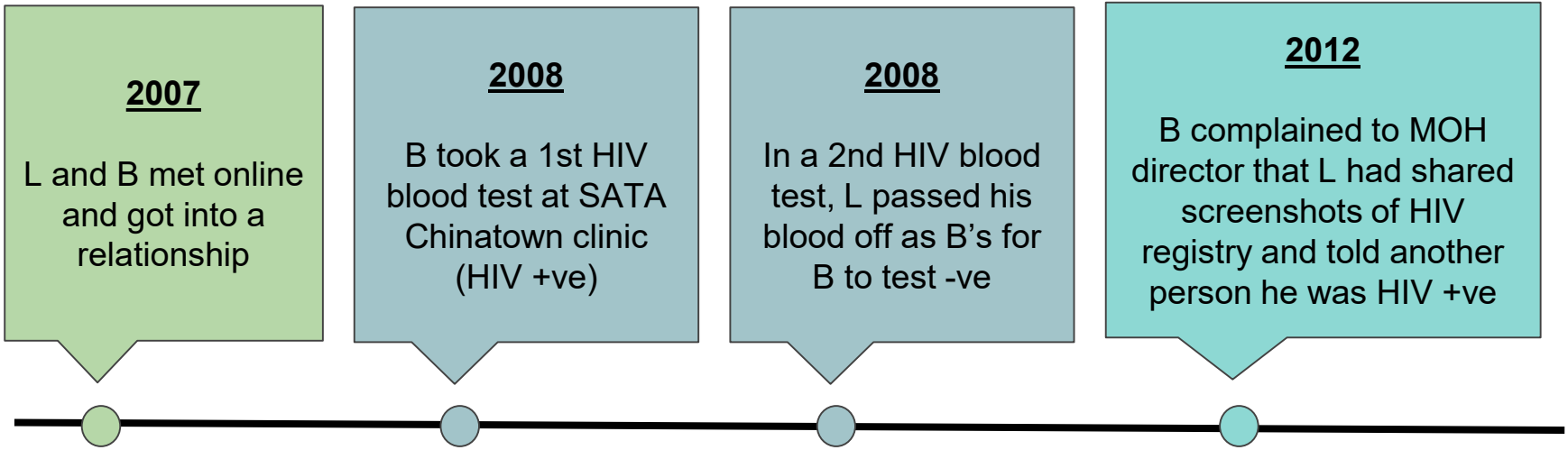
Details include **names**, **ID numbers** , **phone numbers** , **HIV test results** , **related medical information** and **addresses**.

All these information were released online.

# Timeline of events

Legend

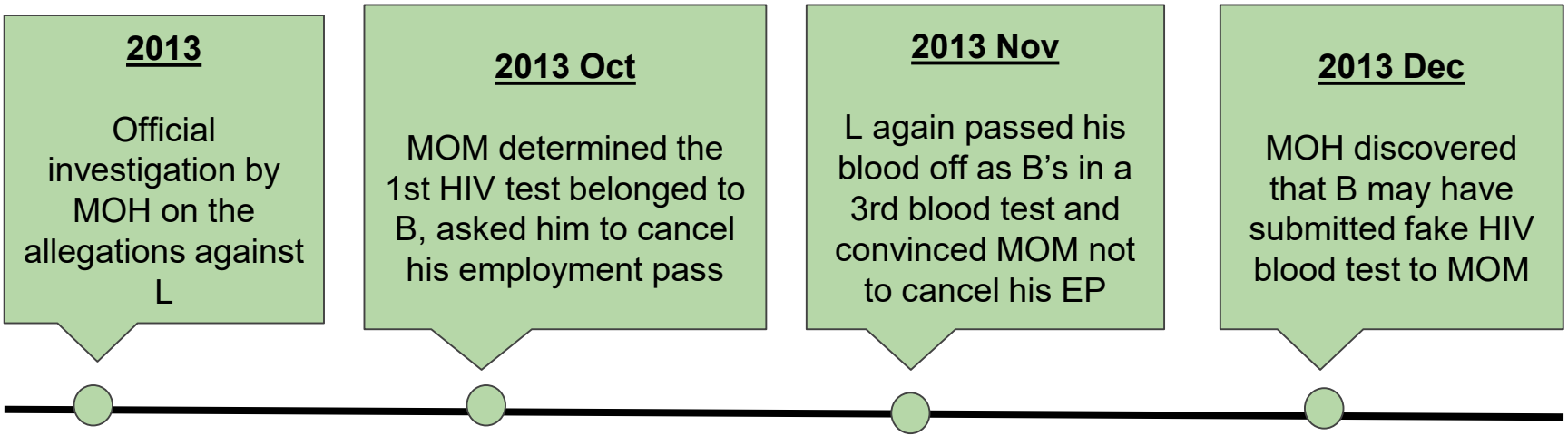
B - Mikhy K Farrera Brochez
L - Ler Teck Siang



# Timeline of events

Legend

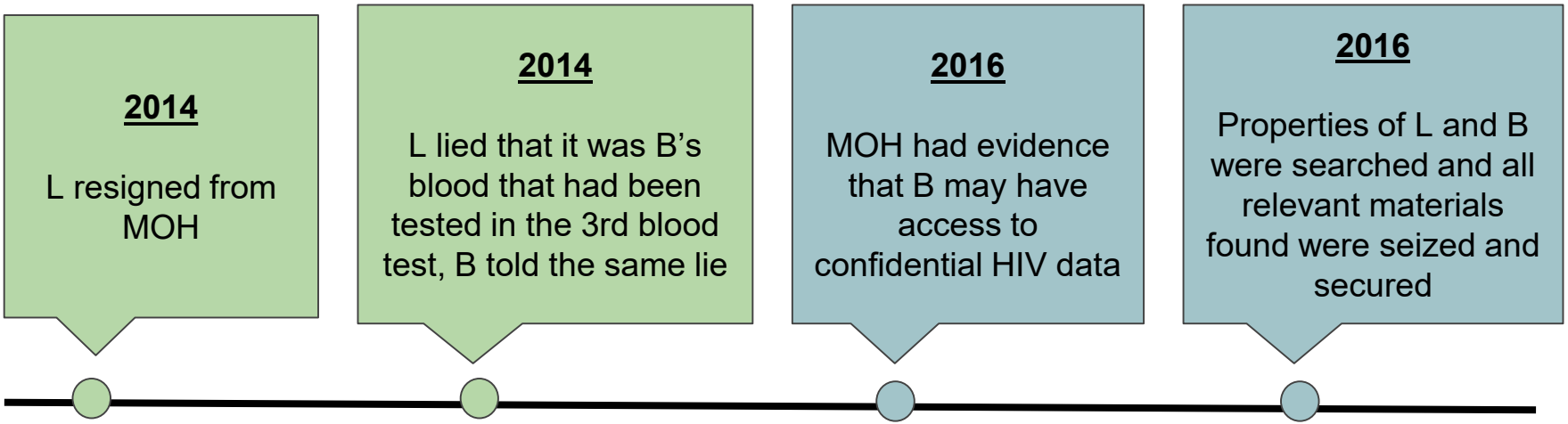
B - Mikhy K Farrera Brochez
L - Ler Teck Siang



# Timeline of events

Legend

B - Mikhy K Farrera Brochez
L - Ler Teck Siang



# The impact of this incident

| | |
|---|---|
| Data | ● 14,200 people diagnosed with HIV were leaked online<br>● Includes name, ID, numbers, phone numbers, addresses<br>● The name, identification number, phone number and address of 2,400 people identified through contact tracing up to May 2007 was also included. |
| HIV individuals | ● Emotional and psychological damage<br>● Many individuals who had kept that HIV status hidden now had to deal with their friends and families knowing about it through the leak<br>● Employers also know about it, causing them to worry about their jobs<br>● Deal with the stigma against HIV-positive individuals |

# The impact of this incident

| | |
|---|---|
| MOH Reputation | ● Brought up many questions about how Singapore uses and safeguards such confidential records.<br>● Effect is amplified as the HIV leak happened after the 2018 Singhealth data breach case. |
| Legal | Ler Teck Siang<br>● 4 penal code charges, 1 OSA charge and 3 MDA charges<br>● Convicted of 4 penal code charges and 2 MDA charges, sentenced to a total of 24 months imprisonment in 2018 and 15 months imprisonment in 2020<br>Mikhy K Farrera Brochez<br>● Total of 23 charges, 4 MDA charges and 19 Penal code charges.<br>● Pleaded guilty to 4 Penal code charges and 2 MDA charges, sentenced to a total of 28 months imprisonment and the remaining 17 charges were taken into consideration<br>● Deported from Singapore after sentence<br>● Extorting Singapore government using the leaked data<br>● Guilty of 3 charges by US and faces maximum jail term of nine years and fine of 750k USD.<br>● Singapore's MOH also has an ongoing civil lawsuit against him in Kentucky, to compel him to delete and return the stolen HIV registry data. |

# Measures by MOH

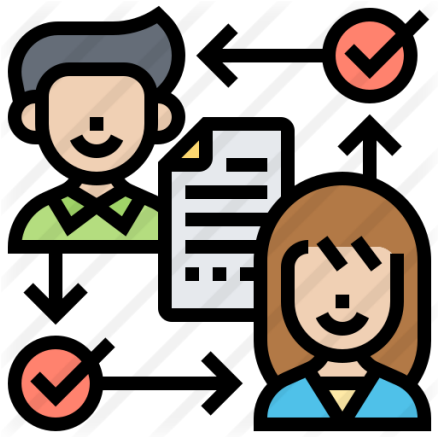
2016:

1. 2 person approval process for downloading and decrypting registry information
2. Special Workstations modified to prevent unauthorised information removal

2017:

3. Disabled the use of unauthorised portable storage devices on portable computers
    a. Government wide policy, not initiated by the MOH

# Measure 1
# 2 Person Approval Process



## Pros

- Similar to NSA's "two -man rule"
- If implemented properly, in theory this should be useful

## Cons

- No specification of level of privilege required
- No specification on how the verification process will be implemented
    - Is there a 2FA to ensure that the risk of stolen passwords / imitation

# Measure 2
# Special Workstations

## Pros

- Physical protection of hardware to deter physical theft of data

## Cons

- Needs more specification on how the locking is implemented and who has access to the keys

# Measure 3
# Portable Storage Device Restrictions

## Pros

- Aids in restricting unauthorized access to official computers

## Cons

- May have implementation difficulties
  - How to determine / track if a storage device is authorised or not
- May result in difficulties or inconveniences with regards to special arrangements like Work From Home arrangements

# CIS Controls V7 Measures and Metrics

Problem: Insider data leak

| Sub-Control | Title | Purpose |
|---|---|---|
| 1.2 | Utilize an Passive Discovery Tool | Detect devices connected to the network |
| 1.5 | Maintain Asset Inventory Information | Track who accessed what, when, whether permission has been granted |
| 1.6 | Address Unauthorised Assets | Remove / Quarantine unauthorized assets |
| 1.7 | Deploy Port Level Access Control | Control devices which can authenticate to the network |

# CIS Controls V7 Measures and Metrics

Problem: Insider data leak

| Sub-Control | Title | Purpose |
|---|---|---|
| 2.6 | Address unapproved software | Remove / Quarantine unauthorized softwares |
| 4.1 | Maintain Inventory of Administrative Accounts | Ensure that only authorized individuals have elevated privileges. |
| 4.2 | Change Default Passwords | |
| 4.3 | Ensure the Use of Dedicated Administrative Accounts | dedicated or secondary account for elevated activities - no emails or internet browsing |

# CIS Controls V7 Measures and Metrics

Problem: Insider data leak

| Sub-Control | Title | Purpose |
|---|---|---|
| 4.4 | Use Multifactor Authentication For All Administrative Access | Prevent stolen passwords / impersonation |
| 4.6 | Use of Dedicated Machines For All Administrative Tasks | No access to internet |
| 4.7 | Limit Access to Script Tools | Prevent running of potentially malicious softwares |
| 4.9 | Log and Alert on Unsuccessful Administrative Account Login | Suspicious activity detection |

# CIS Controls V7 Measures and Metrics

Problem: Insider data leak

| Sub-Control | Title | Purpose |
|---|---|---|
| 8.4 | Configure Anti-Malware Scanning of Removable Devices | anti-malware scan of removable media when inserted or connected |
| 8.5 | Configure Devices Not To Auto-run Content | Configure devices to not auto-run content from removable media |
| 8.6 | Centralize Anti-malware Logging | Capture malware detection events for analysis and alerting |
| 8.7 | Enable DNS Query Logging | Detect hostname lookups for known malicious domains |

# CIS Controls V7 Measures and Metrics

Problem: Insider data leak

| Sub-Control | Title | Purpose |
|---|---|---|
| 13.6 | Encrypt the Hard Drive of All Mobile Devices | Protection against theft / removal of hard drives from official laptops |
| 13.7 | Manage USB Devices | Control list of authorized USBs |
| 13.8* | Manage System's External Removable Media's Read/write Configurations | Some devices should not be allowed to write to external storage devices |
| 13.9 | Encrypt Data on USB Storage Devices | Protection against theft / loss of authorised USBs |

# CIS Controls V7 Measures and Metrics

Problem: Insider data leak

| Sub-Control | Title | Purpose |
|---|---|---|
| 14.6 | Protect Information through Access Control Lists | Control account privilege access |
| 14.9 | Detail Logging for Access or Changes to Sensitive Data | For tracking who access / changed what when |
| 16.8 - 16.10 | Account Management | Close unassociated / dormant and set expiry dates |
| 16.11 | Lock Workstation Sessions After Inactivity | Protection against forgetfulness / toilet breaks |

# CIS Controls V7 Measures and Metrics

Problem: Insider data leak

| Sub-Control | Title | Purpose |
|---|---|---|
| 16.12 | Monitor Attempts to Access Deactivated Accounts | For analysis on potential attacks |
| 17.5 - 17.9 | Training of workforce | Awareness, training and familiarization with dos and don’ts |
| 19.1 - 19.8 | Incident management and reporting | SOPs on management, tracking and dealing with incidents |

# Thank you!