Security Management Practice

Xia Fuxi
Neo Jia Ern
Ng Shu Lin Jane
Jonah Tham Wen Long

ENTER

Warmup

Participate with us pls

Percentage (%) of vulnerabilities remediated within organization-specific time frames

A

Implementation

B

Effectiveness/Efficiency

C

Impact

D

All of the above

Percentage (%) of vulnerabilities remediated within organization-specific time frames

A

Implementation

B

Effectiveness/Efficiency

C

Impact

D

All of the above

Percentage (%) of vulnerabilities remediated within organization-specific time frames

Measure Type	Effectiveness/**Efficiency**
Formula	(Number of vulnerabilities remediated according to POA&M schedule/total number of POA&M-documented vulnerabilities identified through vulnerability scans) *100

Percentage (%) of individuals screened before being granted access to organizational information and information systems

A

Implementation

B

Effectiveness/Efficiency

C

Impact

D

All of the above

Percentage (%) of individuals screened before being granted access to organizational information and information systems

A

Implementation

B

Effectiveness/Efficiency

C

Impact

D

All of the above

Percentage (%) of individuals screened before being granted access to organizational information and information systems

Measure Type	Implementation
Formula	(Number of individuals screened/total number of individuals with access) *100

Brief Case Introduction

Brief summary

January 2019

- ***Jan 22***: MOH notified by police that confidential information from its HIV Registry may have been disclosed by an unauthorised person. It filed a police report the next day.
- **Jan 24**: MOH determined that that the information matched its HIV Registry records up to January 2013 and "worked with the relevant parties to disable access to the information".
- **Jan 26**: The ministry began contacting affected individuals to notify them and render assistance.
- **Jan 28**: MOH went public about data breach.

After investigations, it was found that **Dr Ler Teck Siang** & **Mr Mikhil Ferrera Brochez** were behind the data breach.

What acts has Mr Ler been charged under? (Multiple Response)

A

PDPA

B

Computer Misuse Act

C

Official Secrets Act

D

Penal Code

What acts has Mr Ler been charged under? (Multiple Response)

A

PDPA

B

Computer Misuse Act

C

Official Secrets Act

D

Penal Code

Official Secrets Act

His partner was Ler Teck Siang, a Singaporean doctor who was head of MOH's National Public Health Unit (NPHU) from March 2012 to May 2013 and had access to the HIV Registry for his work. He has been charged under the Official Secrets Act for failing to take reasonable care of confidential information regarding HIV-positive patients.

Penal Code

2 The Respondent's dishonest and fraudulent acts were eventually discovered. On 17 September 2019, the Respondent was convicted in the State Courts after a full trial on four criminal charges for offences under the Penal Code (collectively, the "**Penal Code**

3

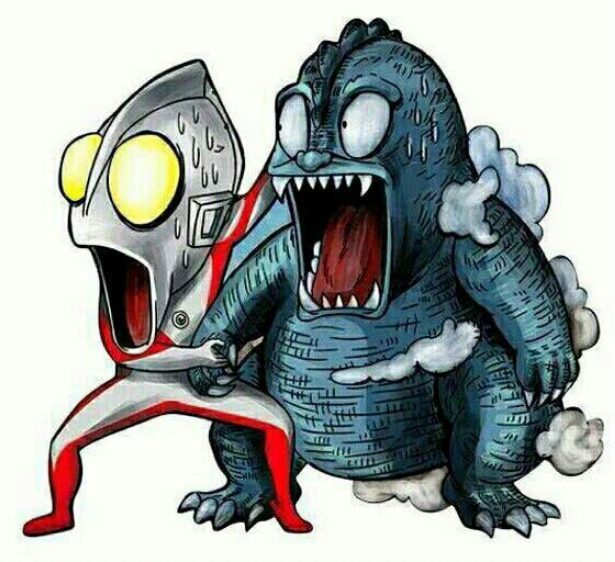
Charges") and was sentenced to a total of 24 months' imprisonment. The Respondent's appeal to the High Court was dismissed. The Respondent's case was well covered in the news at the relevant time.

Discussion questions

Participate with us pls

1a) What data has been compromised? ✕

Confidential information regarding 14.2k individuals diagnosed with HIV up to Jan 2013 were leaked. Information included **names, identification numbers, phone numbers, addresses, HIV test results and related medical information.** Details of 2400 of their contacts were also leaked.



1b) How did the incident happen?

2007

Ler and Brochez met and got into a relationship.

2012

Ler was appointed the head of MOH's National Public Health Unit

2012

Brochez notified MOH about Ler's leak of screen-shots from the HIV Registry

2013

MOH suspected fake blood test results sent by Brochez

2013

Ler lied to investigation manager a bid to halt investigations

1b) How did the incident happen?

May 2016

First time MOH had evidence of Brochez's possession of confidential data

Jun 2016

Ler and Brochez charged in court under various laws

Sep 2016

MOH implemented additional safeguards

May 2018

Brochez sent screenshot of HIV Registry to several Government authorities

2019

MOH confirms data breach

2012

March

- Ler appointed head of the MOH's National Public Health Unit
- Had authority to access information in the HIV Registry as required for his work

2013

December

- MOH suspects Brochez of submitting fake blood tests to MOM
- MOM lodges police report
- Ler and Brochez actively works to halt police investigations

2016

May

- MOH had evidence that Brochez had may have access to confidential HIV data
- Properties of Ler and Brochez were searched and all relevant materials found were seized and secured by the police

June

- **Ler and Brochez charged in court under various laws**

September

- MOH implemented additional safeguards against the mishandling of information by staff
  - Two-person approval
  - Designated workstation

2017

March

- MOH updates security policy to **prevent usage of unauthorised portable storage devices**
- Brochez charged for fraud and drug-related offenses and sent to prison for 28 months

2018

May

- Brochez sent screenshot of 31 records from the HIV Registry to several government authorities
  - Among the 75 given to the authorities in May 2016
  - MOH decided to alert the 31 individuals

September

- Ler convicted of abetting Brochez to cheat and of providing false information to the police and MOH

November

- Ler sentenced to two years' jail

2019

January

- *22 Jan:* MOH notified of potential data breach in HIV registry
- *24 Jan:* MOH confirm Brochez leaked data from HIV registry onto the internet
- *24 Jan:* MOH begins work to disable access to the leaked data
- *26 Jan:* MOH notifies affected individuals
- *28 Jan:* Public is informed regarding the data breach

Timeline of notable events

2012

Ler appointed head of the MOH's National Public Health Unit

2016

MOH had evidence that Brochez may have access to confidential HIV data

2017

Brochez charged for fraud and drug-related offenses

2018

Ler charged under Penal Code and the Official Secrets Act (OSA)

2019

Confidential information from MOH's HIV Registry was disclosed

1c) Impact of this incident

Data

HIV records, Medical Records, Personal Information disclosed

Legal

Ler charged under Penal Code and Official Secrets Act

Organizational

MOH still the number 1 trusted agency :)

Management

New security policies enacted

2) Security Controls

2-person approval process

Designated workstation

Disable use of unauthorised portable storage devices

Data analytics and data governance team set up

2-person approval process

Two people must give authorisation before data can be downloaded and decrypted from HIV registry.

Pros

- Reduces risk of single internal malicious actor from retrieving confidential information
  - Even in this case where outsider has access to staff credentials, this policy would have alerted others

Cons

- May not be as effective when there's multiple malicious actors within the organisation

Designated workstation

A designated workstation specifically configured and locked down to prevent unauthorised information removal for processing of sensitive information from the HIV Registry.

Pros

- Sensitive information cannot be removed without authorisation

Cons

- Reactionary control, cannot be applied to reduce risk on a larger scale

Disable use of unauthorised portable storage devices ✕

Only authorised and encrypted thumb-drives would be allowed on official computers.

Pros

- Ensures that data cannot be easily copied and passed around
- Reduces risk of information leak to due to loss of the devices
- Prevents the installation of malware or viruses through these devices
- Enhanced management of BYOD risks

Cons

- Authorised storage devices are not immune to malware
- Reduced efficiency in daily work
    - Difficult to transfer essential resources from public domain to work computers

Data Analytics and Governance Team

Data Analytics Group and Data Governance Division was formed to give greater attention to data usage and safeguards, to protect and secure access to health sector data.

Pros

- Dedicated department to monitor data flow
- Ensure that best practice data security and governance policies are strictly adhered to

Cons

- Might take a while to reap the benefits
- Major structural shake up required

3) Relevant CIS Controls for MOH

- Asset management
- Logging
- Training
- Incident response
- Access management

3) Relevant CIS Controls for MOH

Asset Management

- 1.6 Address Unauthorized Assets
- 2.5 Integrate Software and Hardware Asset Inventories
- 13.7 Manage USB Devices
- 13.8 Manage System's External Removable Media's Read/write Configurations
- 13.9 Encrypt Data on USB Storage Devices
- 14.8 Encrypt Sensitive Information at Rest

3) Relevant CIS Controls for MOH

Logging

- 6.2 Activate audit logging
- 6.3 Enable detailed logging
- 6.4 Adequate storage for logs
- 6.5 Central log management and analysis
- 6.6 Deploy log analytic tools
- 6.7 Regular review of logs
- 6.8 Regular review of log analytic tools
- 14.9 Enforce logging for access and changes to sensitive data
- 16.12 Monitor Attempts to Access Deactivated Accounts
- 16.13 Alert on Account Login Behavior Deviation

3) Relevant CIS Controls for MOH

Training

- 17.1 Perform a Skills Gap Analysis
- 17.2 Deliver Training to Fill the Skills Gap
- 17.3 Implement a Security Awareness Program
- 17.4 Update Awareness Content Frequently
- 17.7 Train Workforce on Sensitive Data Handling
- 17.8 Train Workforce on Causes of Unintentional Data Exposure
- 17.9 Train Workforce Members on Identifying and Reporting Incidents

3) Relevant CIS Controls for MOH

Incident Response

- 19.1 Document Incident Response Procedures
- 19.2 Assign Job Titles and Duties for Incident Response
- 19.3 Designate Management Personnel to Support Incident Handling
- 19.4 Devise Organization-wide Standards for Reporting Incidents
- 19.5 Maintain Contact Information For Reporting Security
- 19.6 Publish Information Regarding Reporting Computer Anomalies and Incidents
- 19.7 Conduct Periodic Incident Scenario Sessions for Personnel
- 19.8 Create Incident Scoring and Prioritization Schema

3) Relevant CIS Controls for MOH

Access Management

- 14.6 Protect Information through Access Control Lists
- 14.7 Enforce Access Control to Data through Automated Tools
- 16.3 Require Multi-factor Authentication
- 16.11 Lock Workstation Sessions After Inactivity

THANKS!

Do you have any questions?

Done by: **Group 4**
(Fuxi, Jane, Jia Ern, Jonah)