

# Tutorial 7

## Security Management Practice

IS4231 Group 4:

Ho Chong Han Nathaniel

Low Qing Ning

Yuen Si Hao

# MEASUREMENTS FOR PERFORMANCE MANAGEMENT



- Demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures
- Can also be used to examine system-level areas
- Requires data that can be easily obtained

## IMPLEMENTATION

# MEASUREMENTS FOR PERFORMANCE MANAGEME



- Monitor if program-level processes and system-level security controls are implemented correctly, operating as intended, and meeting the desired outcome
- Concentrate on evidence and results of assessments, may require multiple data points
- Effectiveness:
  - Robustness of the result
- Efficiency:
  - Timeliness of result

EFFECTIVENESS /  
EFFICIENCY

# MEASUREMENTS FOR PERFORMANCE MANAGEME



IMPACT

- Articulate the impact of information security on an organization's mission
- Organization specific
- Can be used to quantify:
  - Cost savings
  - Degree of public trust gained/maintained
  - Other mission-related impacts

# MEASUREMENTS FOR PERFORMANCE MANAGEME

- A measurement can contain aspects from all 3 categories
- “Percentage of enterprise operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated”
- Measures both implementation and the effectiveness

# MEASUREMENTS FOR PERFORMANCE MANAGEME

- Type of measures used is also determined by the maturity of the organization's information security program
- Less Mature programs need to develop goals and objectives
- Mature programs use implementation measures to evaluate performance
- More mature programs use effectiveness/efficiency and impact measures



---

# Warm Up Questions

---



Considering 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



Considering 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

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

Field	Data
Measure ID	Vulnerability Measure 1
Goal	<ul style="list-style-type: none"><li>• <i>Strategic Goal:</i> Ensure an environment of comprehensive security and accountability for personnel, facilities, and products.</li><li>• <i>Information Security Goal:</i> Ensure all vulnerabilities are identified and mitigated.</li></ul>
Measure	Percentage (%) of high <sup>13</sup> vulnerabilities mitigated within organizationally defined time periods after discovery NIST SP 800-53 Controls: RA-5; Vulnerability Scanning
Measure Type	Effectiveness/ <b>Efficiency</b>
Formula	(Number of high vulnerabilities identified and mitigated within targeted time frame during the time period /number of high vulnerabilities identified within the time period) *100
Target	This should be a high percentage defined by the organization.

Considering 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

Considering 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

### 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	<ul style="list-style-type: none"><li>• <i>Strategic Goal:</i> Ensure an environment of comprehensive security and accountability for personnel, facilities, and products.</li><li>• <i>Information Security Goal:</i> Ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions.</li></ul>
Measure	Percentage (%) of individuals screened before being granted access to organizational information and information systems  NIST SP 800-53 Controls – AC-2: Account Management and PS-3: Personnel Screening
Measure Type	Implementation
Formula	(Number of individuals screened/total number of individuals with access) *100
Target	This should be a high percentage defined by the organization.

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

- A. PDPA
- B. Computer Misuse Act
- C. Official Secrets Act
- D. Penal Code



---

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

A. PDPA

B. Computer Misuse Act

**C. Official Secrets Act**

**D. Penal Code**

---



7 Brochez was a partner of Ler Teck Siang, a male Singaporean doctor. As the Head of MOH's National Public Health Unit (NPHU) from March 2012 to May 2013, Ler had authority to access information in the HIV Registry as required for his work. Ler resigned in January 2014. He was charged in Court in June 2016 for offences under the Penal Code and the Official Secrets Act (OSA). In September 2018, Ler was convicted of abetting Brochez to

MOH: UNAUTHORISED POSSESSION AND DISCLOSURE OF INFORMATION FROM HIV  
REGISTRY



# Timeline of HIV Leak Case

2007

Ler and Brochez met online  
and got into a relationship

1

2012

- Ler was head of the MOH's National Public Health Unit from March 2012 to May 2013
- Ler was reassigned and access to HIV Registry was terminated

2

# Timeline of HIV Leak Case

## 2016 (May - June)

- First time MOH had evidence that Brochez may have access to confidential HIV data.
- Police report was lodged.
- Properties of Ler and Brochez were searched and all relevant materials found were seized and secured by the police.
- Brochez has sent a pdf file with records to his mother by email.
- According to Ler's charge sheet, he **failed to retain the possession of a thumbdrive** which he has saved the HIV Registry.





---

Do you think there was a policy implemented for encryption of storage devices?

The policy on encrypted storage devices was not in place until **2017**.

---





---

The old policy was that if data was stored on a storage device, you must protect the device itself, access to data, and ensure that it is with you at all times. Is this a successful policy?

#### Successful Policy Characteristics

- Endorsed
- Relevant
- Realistic
- Attainable
- Adaptable
- Enforceable
- Inclusive



The old policy was that if data was stored on a storage device, you must protect the device itself, access to data, and ensure that it is with you at all times. Is this a successful policy?


No, the following characteristics are not met:

- Endorsed
- Relevant
- **Realistic**
- **Attainable**
- Adaptable
- **Enforceable**
- Inclusive

Should MOH have informed the affected persons and public at this point (in 2016), knowing the possibility that Brochez could have possess more records? Why?

**MOH's Approach**


- Need to consider the impact on the persons living with HIV
- Felt that informing individuals or public cause more harm
  - Deeply emotional, personal matter. Compelled to reveal to family members, cause anxiety and distress
- Possibility of affecting relationships, change lives
- Did not inform anyone




---

Should MOH have informed the affected persons and public at this point (in 2016), knowing the possibility that Brochez could have possess more records? Why?

Our Opinions


- Need to be transparent with the individuals, it is their data
  - May further harm them if data used against them in future
  - Just inform the individuals
- 
- 



---

Was this due to the social stigma on HIV? Should there be any difference in notifying the parties / public as compared to the SingHealth data breach?

**Our Opinions**

- Should inform the affected individuals or public just like any other data breaches
  - Should not create exceptions for themselves
- 
- 



# Timeline of HIV Leak Case

2018

- April: Brochez was deported from Singapore after completing his sentence.
- May:
  - Brochez sent screenshot of 31 records from the HIV Registry to several government authorities.
  - MOH decided to alert the 31 individuals.

# Timeline of HIV Leak Case

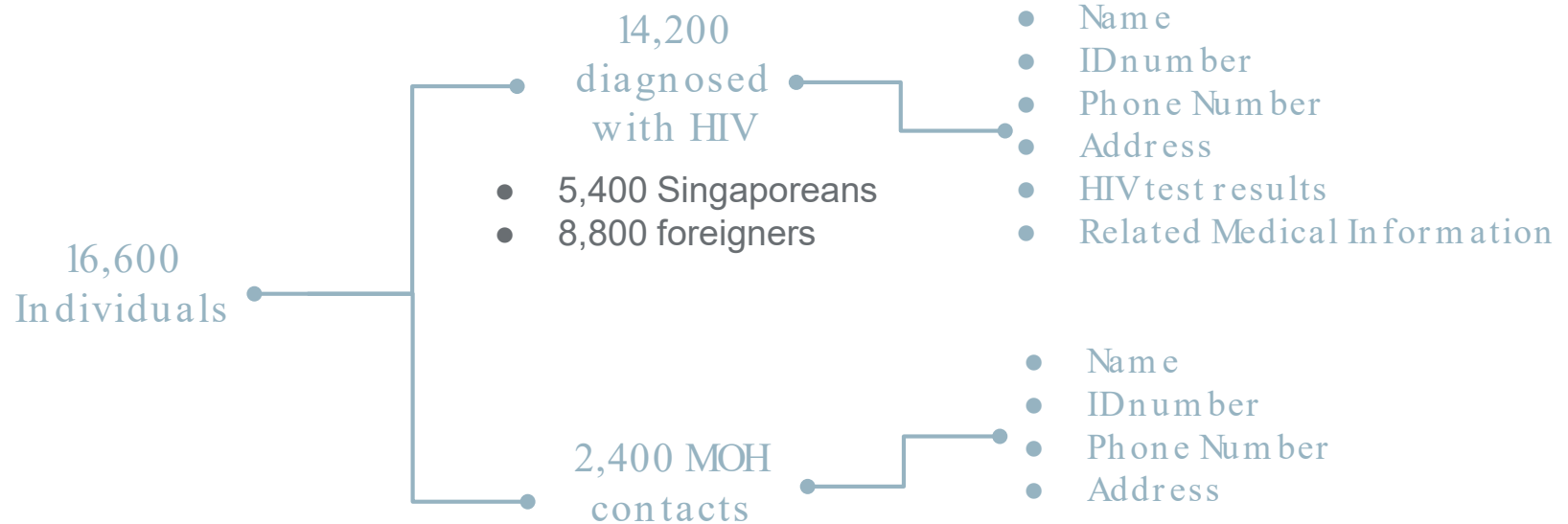
2019

- Brochez still has the HIV Registry records, put them online and sent the link to a non-government party.
  - Risk of identity exposure increased significantly.
- Jan 22: MOH notified by police that confidential information from its HIV Registry may have been disclosed by an unauthorized 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.



What data has been compromised?

# What data has been compromised?





---

# Impact of This Incident

# Impact of This Incident



Sold or used for  
blackmail



Anxiety and Stress



Relationships and  
Job Prospects



Public trust in  
MOH



Anger Directed at  
Medical Social Workers



Drop in care service  
return rates

# Security Controls implemented (2016)

- MOH's Chief Data Officer (CDO) conducted a data security review on MPHU
- Elevating the authority for downloading and decrypting registry data to the level of Director of Communicable Diseases Division (CDD) or higher
- A two-person approval process was implemented to download and decrypt registry information to ensure that the information cannot be accessed by a single individual
- A workstation — specifically configured and locked down to prevent unauthorized information removal — was designated for the processing of sensitive information from the HIV Registry

# Effectiveness of Security Controls implemented (2016)

Security Controls	Comments
MOH's CDO conducted data security review	Allows presence of champion and top-down risk based approach.
Elevating the authority for downloading and decrypting registry data	Reduce the number of privileged access.  However, this still does allow privileged access to higher authority which might not solve the issue.
Two-person approval process	Allows colleagues to monitor the access of the data.
Specially configured and locked down workstation	Ensures that information could not be retrieved easily.



# Security Controls implemented (2017)

- MOH disabled the use of unauthorized portable storage devices on portable computers as part of a government-wide policy (Only allow the use of authorized and encrypted thumb drives)

# Effectiveness of Security Controls implemented (2017)

Security Controls	Comments
Disable the use of unauthorized portable storage devices and only allow the use if authorized and encrypted	<p>Portable storage devices are usually unprotected and cannot be guaranteed to keep safe 24/7.</p> <p>Authorized and encrypted storage devices ensures that even if storage devices is stolen or misused, potential data leak is minimized.</p>

# Security Controls implemented (2018)

- Setup of Data Analytics Group in MOH
  - Data Governance Division to formulate policies and guidelines for MOH and its agencies to protect and secure access to health sector data in accordance with Government IM and other sectoral guidelines
- Specific mandate and team to investigate compliance and audit of data access and use on the ground

# Effectiveness of Security Controls implemented (2018)

Security Controls	Comments
Setup of Data Analytics Group in MOH, inclusive of Data Governance Division that formulate policies and guidelines for MOH in accordance with Government IM and other sectoral guidelines.	<p>Ensures that there are successful policies and guidelines for MOH to follow closely.</p> <p>However, this does not ensure the effectiveness of the policies as enforcement is difficult.</p>
Specific mandate and team to investigate compliance and audit of data access and use on the ground	Good to have a specific team to ensure the policies are adhered to.



---

What are the highly relevant controls you would recommend to MOH?

# What are the highly relevant controls you would recommend to MOH?

## Our Opinions

- Control 13: Data Protection
- Control 14: Controlled Access based on the Need to Know
- Control 17: Implement a Security Awareness and Training Program

# What are the highly relevant controls you would recommend to MOH?

## Control 13: Data Protection

- 13.1 - Maintain an Inventory Sensitive Information
- 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

# Control 13 - Data Protection

Sub-Controls	Measures
13.1 - Maintain an Inventory Sensitive Information	Does the organization maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider?



# Control 13 - Data Protection

Sub-Controls	Measures
13.7 - Manage USB Devices	What percentage of the organization's hardware assets are not configured to only allow the use of specific USB devices?
13.8 - Manage System's External Removable Media's Read/write Configurations	What percentage of the organization's hardware assets are not configured not to write data to USB storage devices, if there is no business need for supporting such devices?
13.9 - Encrypt Data on USB Storage Devices	What percentage of the organization's hardware assets are not configured to encrypt all data stored on USB devices?

# What are the highly relevant measures you would recommend to MOH?

## Control 14: Controlled Access based on the Need to Know

- 14.5 - Utilize an Active Discovery Tool to Identify Sensitive Data
- 14.6 - Protect Information through Access Control Lists
- 14.7 - Enforce Access Control to Data through Automated Tools
- 14.8 - Encrypt Sensitive Information at Rest
- 14.9 - Enforce Detail Logging for Access or Changes to Sensitive Data

# Control 14 - Control Access Based on the Need to Know

Sub-Controls	Measures
14.5 - Utilize an Active Discovery Tool to Identify Sensitive Data	What percentage of the organization's assets have not been scanned by an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems?
14.6 - Protect Information through Access Control Lists	What percentage of the organization's hardware assets have not been configured with appropriate file system, network share, claims, application, or database specific access control lists?

# Control 14 - Control Access Based on the Need to Know

Sub-Controls	Measures
14.7 - Enforce Access Control to Data through Automated Tools	What percentage of the organizations systems do not use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system?
14.8 - Encrypt Sensitive Information at Rest	What percentage of the organization's sensitive information is not encrypted at rest and requires a secondary authentication mechanism not integrated into the operating system, in order to access the information?
14.9 - Enforce Detail Logging for Access or Changes to Sensitive Data	What percentage of the organization's sensitive information does not require detailed audit logging when the data is accessed?

# What are the highly relevant measures you would recommend to MOH?

## Control 17: Implement a Security Awareness and Training Program

- 17.1 - Perform a Skills Gap Analysis
- 17.2 - Deliver Training to Fill the Skills Gap
- 17.3 - Implement a Security Awareness Program
- 17.5 - Train Workforce on Secure Authentication
- 17.6 - Train Workforce on Identifying Social Engineering Attacks
- 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

# Control 17 - Implement a Security Awareness and Training Program

Sub-Controls	Measures
17.1 - Perform a Skills Gap Analysis	Has the organization performed a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.
17.2 - Deliver Training to Fill the Skills Gap	Has the organization delivered training to address the skills gap identified to positively impact workforce members' security behavior.

# Control 17 - Implement a Security Awareness and Training Program

Sub-Controls	Measures
17.3 - Implement a Security Awareness Program	Has the organization created a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.
17.5 - Train Workforce on Secure Authentication	Has the organization trained workforce members on the importance of enabling and utilizing secure authentication.

# Control 17 - Implement a Security Awareness and Training Program

Sub-Controls	Measures
17.6 - Train Workforce on Identifying Social Engineering Attacks	Has the organization trained the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.
17.7 - Train Workforce on Sensitive Data Handling	Has the organization trained workforce on how to identify and properly store, transfer, archive and destroy sensitive information.



# Control 17 - Implement a Security Awareness and Training Program

Sub-Controls	Measures
17.8 - Train Workforce on Causes of Unintentional Data Exposure	Has the organization trained workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
17.9 - Train Workforce Members on Identifying and Reporting Incidents	Has the organization trained employees to be able to identify the most common indicators of an incident and be able to report such an incident.

The background of the slide features abstract, painterly textures. The top section has warm, earthy tones like beige and light brown. The bottom section transitions into cooler tones, including light blues and greys. The central area is a clean, white space where the text is located.

# THANKS!

Do you have any questions?

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik**