Tutorial 7: Security Management Practices

Group Led Discussion Session 4 – Group 4

Purpose:
- We believe in **peer teaching** philosophy in student learning process and group led discussion is an effective way. It is also a good opportunity for students to practice presentation and discussion leading skills. When we talk about group led discussion, it is not just a formal PowerPoint presentation where presenters directly present to the audience. We expect the team would stimulate meaningful and lively interaction and discussion among students.

Session Guidelines:

For the team:
- The team should pay attention to the time management (e.g., around 45 mins)
- The team could choose different ways (e.g., PowerPoint slides, whiteboard, game activities) to better facilitate them leading the discussion. Please send your **discussion documents (e.g., PowerPoint slides) to me before the tutorial session day starts.** You can still make slight changes after that.
    - For **T1** and **T2**, pls send to me by **Tuesday**.
    - For **T3**, pls send to me by **Thursday**.
- Every member is required to present or lead the discussion.
- The team should carefully research on the tutorial tasks and prepare their own findings beforehand, so as to better lead the discussion.
- All team members should be **visually present** (i.e., turn on device camera) to lead the discussion, so as to increase visual presence and interactivity in class.
- All team members will be set as **co-host** of the meeting, so you have full control of the discussion session.

For the rest class:
- Should also research and work on the tutorial questions and prepare your findings
- Actively share your findings and opinions in class

For everyone in the class:
- Complete that week's tutorial quiz questions on LumiNUS-Quiz before the tutorial session starts.
    - Submission deadline:
        - **By that week's Wed noon, before that week's tutorial session starts**.
    - Grading
        - Your submission will be used to evaluate your participation in team-ted tutorial sessions.

Discussion

Background

Singapore HIV Data Breach

"SINGAPORE — Health Minister Gan Kim Yong revealed new details on the leak of Singapore's human immunodeficiency virus (HIV) Registry in his ministerial statement in Parliament on Tuesday (Feb 12, 2019).

The data breach – announced by the Ministry of Health (MOH) on Jan 28 2019– was the work of HIV-positive American Mikhy K Farrera Brochez, whose partner Ler Teck Siang was head of the ministry's National Public Health Unit from March 2012 to May 2013. Ler had access to the HIV Registry.

The HIV Registry leak affected 14,200 individuals diagnosed with the human immunodeficiency virus and 2,400 of their contacts."

- Detailed timeline:
  https://www.todayonline.com/singapore/hiv-data-leak-timeline-events

- Gan Kim Yong on Singapore HIV data leak | Full ministerial statement and Q&A:
  https://www.youtube.com/watch?v=ccvCP-06Uo8

- Unauthorized possession and disclosure of information from HIV registry
  https://www.moh.gov.sg/news-highlights/details/unauthorised-possession-and-disclosure-of-information-from-hiv-registry

Part I: Warm up questions (submit your answers via LumiNUS-quiz by Wed noon)

1) 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.

2) 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.

3) What act has Mr Ler been charged under? (Pls select all the options that apply)
    a. PDPA
    b. Computer Misuse Act
    c. Official Secrets Act
    d. Penal Code

Part II: Discussion questions

1. Introduce this case:
    1) What data has been compromised?
    2) How did this incident happen?
    3) The impact of this incident

2. After this incident, what security controls have been taken by MOH to improve internal information security management? Comments on the effectiveness of each implemented control.

3. Read *CIS Controls V7 Measures and Metrics*, Considering the above incident in MOH, what measures from all the candidate measures you think are highly relevant and would recommend MOH to adopt to better monitor and evaluate its InfoSec performance onwards?