IS4231 Information Security Management, Semester 1, AY21/22

Tutorial 6: InfoSec Policies and Governance

Group Led Discussion Session 3 – Group 3

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

Back in April 2017, a breach of the IT networks of NUS and NTU has been discovered. Intrusions into NTU's networks were detected when the university ran its regular checks on its systems on 19th April. NUS detected an unauthorized intrusion into its IT systems on 11th April, during cybersecurity assessments by external consultants who had been engaged to strengthen its cyber defense.

In each instance, NTU and NUS promptly alerted the Cyber Security Agency of Singapore (CSA) who has been assisting the affected universities to conduct forensic investigations to understand the nature and extent of these attacks. Based on investigations, both the attacks were the work of Advanced Persistent Threat (APT) actors. They are carefully planned and are not the work of casual hackers. The objective may be to steal information related to government or research. There is no evidence that information or data related to students was being targeted. However, as the universities' systems are separate from government IT systems, the extent of the APTs' activities appear to be limited. The daily operations of both universities, including critical IT systems such as student admissions and examinations databases, were not affected. Nonetheless, NUS and NTU have increased vigilance, and adopted additional security measures beyond those already in place.

After the incident, NUS continues to improve their information security policy and governance program.

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

1) According to NUS IT Security Policy, users should familiarize themselves with NUS IT Security Policy and all other relevant security standards and procedures. Though in case by case situations, ignorance will be accepted as a valid reason for non-compliance.
    a. True
    b. False

2) According to NUS IT Security Policy, it adopts need-to-know and least privilege access control principles. Therefore, by default, School Dean should have access to each faculty member's account on LumiNUS and evaluate whether the grading is appropriately done, as the rank of School Dean is higher than faculty members' rank in the organization.
    a. True
    b. False

3) According to NUS IT Security Policy, dual control over the issue of access cards/keys to "secured areas" shall be in place.
    a. True
    b. False

4) According to NUS IT Security Policy, non-critical data should be backed up daily and stored in a secured off-site location.
    a. True
    b. False

5) The agreement between NUS and suppliers may include which of the following requirements? (please select all the options that apply)
    a. Compliance obligations
    b. Service level agreement (e.g., availability, response time)
    c. Right to monitor and review (e.g., privilege accounts, accesses, system performances, logs, configurations, transactions)
    d. Right to audit (including sub-contractor)

Part II: Discussion questions

1. Introduce the following roles and corresponding responsibilities.
    1) Data Owner
    2) Data Stewards
    3) Data Managers
    4) Data Custodian
    5) Data Users
    6) Data Governance Team

2. Using the seven successful policy characteristics to evaluate NUS IT Security Policy, which characteristic causes the most doubt/challenge for this policy's success?
    1) Endorsed
    2) Relevant

3) Realistic
4) Attainable
5) Adaptable
6) Enforceable
7) Inclusive

3. Read the section of Information Security Governance Maturity Model in "Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition" from ISACA (i.e., Information Systems Audit and Control Association) (p.36-p.39) and answer the following questions:
    1) Briefly introduce the model
    2) Based on your reading of NUS information security related policies and your daily observation on InfoSec management on campus, assess NUS information security governance management, which maturity level does NUS meet?