IS4231 Information Security Management, Semester 1, AY21/22

Tutorial 8: Security Management Models

Group Led Discussion Session 5 – Group 5

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

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

1) Considering why a certain information system/infosec program could be PCI DSS compliant but not secured, which of the following is a potential reason? (Pls select all the options that apply)
    a. The effectiveness of Self-assessment compliant is with doubt.
    b. Typically, QSAs may only review a sample of system components.
    c. The system could be compliant at the examination point but failed to keep compliant along the way.
    d. QSAs' professionalism may be with doubt.

2) Theoretically, which of the following merchants does *not* need to comply with PCI standards?
    a. Starbucks
    b. Square POS
    c. FavePay
    d. None of the above

3) Considering the seven EALs, which of the following products may be more likely to get itself examined against EAL 7 (i.e., Formally Verified Design and Tested) requirements?
    a. Commercial firewall
    b. Chips for military usage
    c. Digital signature solution
    d. Key management system

Part II: Discussion questions

1. PCI DSS Requirements

In Target data breach case, Target had successfully passed a PCI-DSS audit a few months prior to the breach. From the reports, Security Firm Trustwave, the qualified security assessor hired by Target, conducted the audit for Target and certified Target as PCI-DSS compliant. After the breach happened, a few banks filed lawsuits against both Target and Trustwave.

- Recommended resources:
    - "Target, security auditor Trustwave are sued over data breach"
        - https://www.reuters.com/article/us-target-trustwave-lawsuit-idUKBREA2P0B020140326
    - Compliant but not Secure: Why PCI-Certified Companies Are Being Breached
        - https://csiac.org/articles/compliant-but-not-secure-why-pci-certified-companies-are-being-breached/
    - The Prioritized Approach to Pursue PCI DSS Compliance v3.2.1
    - PCI-DSS SAQ Instructions and Guidelines v3.2.1

Based on the information we have discussed from the previous tutorial discussion, discuss the following questions:

1) What are the requirements in PCI DSS v3.2.1 that Target might have failed to comply with before the breach? (e.g., 8.3. Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication).

2) Considering the business model of Target, if Target planned to conduct self-assessment for compliance purpose, which Self-Assessment Questionnaire (SAQ) Target should use to do self-assessment (e.g., A, A-EP)?

2. Common Criteria

Common Criteria, as an information security evaluation model, is widely accepted by industry players and is the de facto standard for cybersecurity standard certification around the world.

- Recommended resources:
  - Common Criteria
    - https://www.commoncriteriaportal.org/
  - Protection Profile
    - https://www.niap-ccevs.org/Profile/PP.cfm

1) In CC certified products list, under Detection Devices and Systems Section, we notice that two IDPS systems with different EALs achieved:

   - Trend Micro Deep Security 11.0 (EAL2+)
   - LogPoint 5.2.5 (EAL3+)

   Source: https://www.commoncriteriaportal.org/products/

   Can we base on the different EALs received by these two products and draw the conclusion that *product b is more secured than product a*? Provide your justifications.

2) Recently, in addition to the traditional seven EALs, a new compliance level has been established and it is PP Compliant. This PP Compliant quickly received wide adoption in the market and welcomed by the business players. Introduce what is PP Compliant and its advantages.