Tutorial 5: InfoSec Program at Zoom Video Communication

Group Led Discussion Session 2 – Group 2

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

The Federal Trade Commission has conducted an investigation of certain acts and practices of Zoom Video Communication, Inc. in 2020. The investigation results showed that the video conferencing provider engaged in a series of deceptive and unfair practices that undermined the security of its users.

Zoom has agreed to a requirement to establish and implement a comprehensive security program, a prohibition on privacy and security misrepresentations, and other detailed and specific relief to protect it user base.

In the compliant, the FTC alleged that, since at least 2016, Zoom misled users by touting that it offered "end-to-end, 256-bit encryption" to secure users' communications, when in fact it provides a lower level of security. In addition, the FTC alleges, Zoom maintained the cryptographic keys that could allow Zoom to access the content of its customers' meetings, and secured its Zoom Meetings, in part, with a lower level of encryption than promised. Zoom's misleading claims gave users a false sense of security, especially for those who used the company's platform to discuss sensitive topics such as health and financial information.

Furthermore, according to the FTC's compliant, Zoom also misled some users who wanted to store recorded meetings on the company's cloud storage by falsely claiming that those meetings were encrypted immediately after the meeting ended. Instead, some recordings allegedly were stored unencrypted for up to 60 days on Zoom's servers before being transferred to its secure cloud storage.

More unfair and insecure practices were identified in Zoom's operations, which revealed problems in Zoom's information security program as well as its business operations.

In Feb, 2021, The FTC finalized a settlement with Zoom. The final order requires Zoom to implement a comprehensive security program.

- Recommended resources:
  - FTC Requires Zoom to Enhance its Security Practices as Part of Settlement
    - https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement
  - FTC Gives Final Approval to Settlement with Zoom over Allegations the Company Misled Consumers about Its Data Security Practices
    - https://www.ftc.gov/news-events/press-releases/2021/02/ftc-gives-final-approval-settlement-zoom-over-allegations-company
  - FTC Final Order on Zoom
    - https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf
  - The Facts Around Zoom and Encryption for Meetings/Webinars
    - https://blog.zoom.us/facts-around-zoom-encryption-for-meetings-webinars/

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

1) Considering the misleading and misrepresented information Zoom claimed on its offered videoconferencing services, the FTC commission had reason to believe that Zoom has violated the Federal Trade Commission Act. In Singapore, it would be more likely to be charged under what law?
    a. PDPA
    b. Cybersecurity Act
    c. Consumer Protection Act
    d. Competition Act

2) Based on the Final Order from the FTC, what information is *not* considered as "Covered Information"?
    a. Screen name
    b. Chat transcripts
    c. Processor serial number
    d. None of the above.

3) In the FTC's Final Order, the design and implementation of security measures (i.e., policies, procedures, and technical) follows what kind of approach?
    a. User based
    b. Cost based
    c. Risk based
    d. Volume based

Part II: Discussion questions

1) According to the FTC's investigation result, what were the deceptive and unfair practices of Zoom that undermined the security of its users?

2) Based on the FTC's Final Order, what is the mandated comprehensive security program for Zoom to establish, implement, and maintain?

3) Read ISO27k Toolkit ISMS Auditing Guideline Appendix A – Generic Information Security Audit Checklist. Map the detailed requirements from the mandated security program to this checklist.

4) In the Final Order, a senior corporate manger, or if no such senior corporate manager exists, a senior officer of Zoom responsible for Respondent's Information security program is required to submit an annual certification to the Commission. Comments on the purpose and effectiveness of such internal certification arrangement from an information security management perspective.