IS4231 Information Security Management, Semester 1, AY21/22

Tutorial 1: Introduction to InfoSec

1. Team formation
    - Form into 5 teams

2. Discussions

Case background:
http://www.straitstimes.com/singapore/courts-crime/smu-student-who-deleted-exam-scripts-for-fear-of-doing-badly-sentenced-to-2

Additional reading:
https://en.wikipedia.org/wiki/Hardware_keylogger

1) Use C.I.A. triad to evaluate what information characteristics have been sacrificed in the case.
    - Confidentiality
    - Integrity
    - Availability

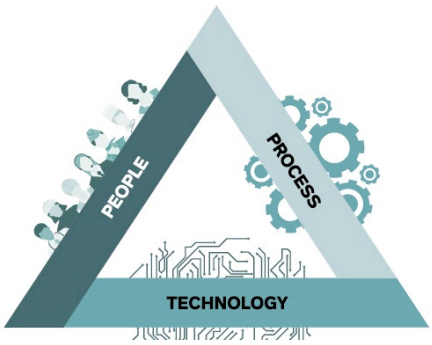
2) Use C.I.A triad extension to evaluate whether data privacy has been compromised and what system characteristics were weak.
    - Privacy
    - Identification
    - Authentication
    - Authorization
    - Accountability

3) Considering this data breach attack case and looking at the bellowing 12 general categories of threats to information security, what threat categories does this attack reflect?
    a. Compromises to Intellectual Property
    b. Deviations in Quality of Service
    c. Espionage or Trespass
    d. Forces of Nature
    e. Human Error or Failure
    f. Information Extortion
    g. Sabotage or Vandalism
    h. Software Attacks
    i. Technical Hardware Failures
    j. Technical Software Failures
    k. Technological Obsolescence
    l. Theft

Table 1-1 The 12 Categories of Threats to Information Security[5]

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

4) Use Trifecta of People, Process, and Technology model to evaluate the original InfoSec management condition of SMU. Identify the vulnerabilities there.



5) Research on what remediation security controls had been taken by SMU after this incident happened. Comments on each control's effectiveness in defending against such hardware keylogger attack. Propose additional solutions that you think are effective.