CAB240 Information Security - Semester 2 2017
Mobile Phone Security Investigation Report
Part II - Task Requirements

This task is an investigation of information security issues associated with your personal mobile phone. Your report has two related parts. The focus of your analysis in:

- **Part I** was examining your phone and your use of it, to identify relevant information security threats and vulnerabilities and identify risks.
- **Part II** is countermeasures to mitigate the risks you identified in Part I. This component builds on the report you submitted for Part I.

For each information security issue discussed in Part I, you will need to find resources that outline control measures that could be applied to prevent the issue or reduce the level of harm. Recall the NSTISSI 4011 cube from Lecture 1. Control measures can involve technology; policy and practices; or education, training and awareness.

NOTE: If you identified a similar issue several times in your Part I submission (say, confidentiality breaches for multiple issues), provide different means of dealing with this in your Part II submission, rather than providing the same control measure multiple times.

PART II Task requirements (and page length guidelines):
Your report should consist of the following sections:

1. An *introduction* giving a very brief description of your information assets, an overview of your use of the device, and a statement of the information security issues you examined in Part I (summarize Part I Sections 1 and 2 into 1 page or less).
2. A brief summary of any *information security issues related to user privacy* revealed in your review of an app privacy policy in Part I Section 3, and discussion of control measures that could be used to address these (1-2 pages).
3. A report on a control measure that could mitigate the *information security issues associated with a mobile device application* you discussed in Part I Section 4 (1 page).
    a. Briefly explain what the control measure is and how it works.
    b. Is it preventive, detective or corrective?
    c. To what degree does it protect the asset? Does it reduce the likelihood or consequence of an incident?
    d. Are there any limitations or other impact (for example, on efficiency, battery power, user experience, technical expertise requirements of user, …)?
4. A report on control measures that could be applied to mitigate the *information security issues associated with the mobile device operating system* discussed in Part I Section 5 (1-2 pages).
    a. Briefly explain what the control measure is and how it works.
    b. Is it preventive, detective or corrective?
    c. To what degree does it protect the asset? Does it reduce likelihood or consequence of an incident?
    d. Are there limitations or other impact (for example, who can implement the control – manufacturer, vendor, user, - and does it impact efficiency, battery power, …)?

5. A report on control measures that could be applied to mitigate the *information security issues associated with user behaviour* discussed in Part I Section 6 (1-2 pages).
    a. Briefly explain what the control measure is and how it works.
    b. Is it preventive, detective or corrective?
    c. To what degree does it protect the asset? Does it reduce likelihood or consequence of an incident?
    d. Are there limitations or other impact (for example, does this require technical expertise or competence of the user, reduce efficiency of other processes, or introduce additional risk, …)?.
6. A report on control measures that could be applied to mitigate the *information security issues associated with physical threats to mobile devices* discussed in Part I Section 7 (1-2 pages).
    a. Briefly explain what the control measure is and how it works.
    b. Is it preventive, detective or corrective?
    c. To what degree does it protect the asset? Does it reduce likelihood or consequence of an incident?
    d. Are there any limitations or other impact (for example, does this require additional equipment, or alter the user experience, …)?
7. *Conclusion* (1 page).
    a. Relate the application of the control measures to the identified information security issues (how much does it alter the risk, and how difficult/costly/time consuming will it be to do), and
    b. Summarize the resulting information security position for your mobile device, if the control measures are applied.
8. *Reference list*.

Academic writing
An important aspect of this assessment task is locating relevant information, either in online resources or in print media. Write your report in your own words. **Do not just 'cut and paste' or copy information from any source into the body of your report: that is plagiarism (a breach of academic integrity) and is not acceptable in Australian universities**. If a breach is detected, the Unit Coordinator must notify the Faculty Academic Integrity Committee, and the penalties imposed may be severe (See QUT MOPP for details). **In previous years, students have failed this unit as a result of the applied penalty.** A useful guide to referencing, citation and report writing is: http://www.citewrite.qut.edu.au/ . QUT librarians will also provide assistance; check the QUT Library homepage for links.

Report presentation
Please include the CAB240 unit code and your name and student number in the header or footer of each page. Use 12 point sized font. A template for Part II Sections 2-6 is provided.

Report submission
Electronic submission of a single file is via the Turnitin link on the CAB240 blackboard site. Be sure to use the Part II link.

Under QUT's current Late Assessment policy, late submissions without an approved extension will receive a mark of 0 (so do submit before the deadline!).