# Peer review assignment block 3 group 5

**Summary of the assignment**

This paper focusses on two Android application markets, which are located in China: Baidu and 360 Mobile Assistant. Here, the official Android application market was blocked mid-2014 and the alternative markets do not have much options regarding the security of the content. The previous assignment has shown that the majority of applications in these markets contain malicious code. The app markets owners (APO) are therefore considered the problem owners. They can reduce their risks by implementing control strategies or/and insurance. To minimize risk at every stage, a mixed risk strategy is preferred. However, next to the APOs, the Chinese government, consumers and app developers also part of the ecosystem. Since they all have their own objectives, they will likely implement their own risk strategies and affect the app marketplace security problem.

The paper ends with calculating the return on security investment of Google’s Vulnerability Rewards Program in which Android took part.

**List of strengths of the assignment**

* Nice that you refer to the previous assignment in the introduction
* “Difference in Security Performance of the Metrics” section is written well. It clearly shows the difference between the different application markets and their objectives.
* In the risk strategy section, all different strategies and its application to the case are explained well. Especially the reflection on the different strategies is a useful addition.
* The different chapters fit well together. It is a consistent story. For example the section “Actor’s risk strategies” is linked well to the “Risk strategies”

**List of major issues**

* In the section *Additional actors who influence the security issues* the attackers could have been mentioned, since there strategies are described in the section *Actors’ risk strategies*.
* In the RoSI section, you used discrete numbers. Instead it would be better to use ranges (e.g. the impact is $60.000-140.000/incident) and a certain probability distribution. If you cannot find the data, you can make assumptions based on references.
* In the RoSI section, a conclusion or reflection on the calculated value is missing. What does a RoSI of -0.6 mean? And what is the reliability of the value?

**List of minor issues**

* Section “The problem owner” is difficult to read, because of long sentences and incorrect use of singular and plural
* Page 3, section *Difference in Security Performance of the Metrics*: “Although there are some limitations in our results due to how VirusTotal get the malware information, the difference is still shocking.” Explain how VirusTotal gets the malware information.
* Page 3, section *Difference in Security Performance of the Metrics*: Try to avoid words like “enormously” and “shocking”. Instead you can (objectively) mention 400 times more.
* Page 4, third line: ???? instead of year.
* Page 5, section *Competitors*: “The review criteria can be found here: https://developer.apple.com/app-store/ review/guidelines/”. Refer to the website in APA style, like you do throughout the rest of the paper.
* Page 10, use a caption for the table
* Page 10, “One year later after the introduction of the program, in [https://security.googleblog.com/2016/06/ one-year-of-android-security-rewards.html] Google proudly show some of the program results:” be consistent in your referencing
* In the *RoSI* section, the calculation is difficult to read. You can use Latex or an equation editor to improve the readability.
* Page 5 section *Strategy* and page 6 *attackers*, the title is on another page than the content of the section.
* 20016 ipv 2016
* Try to avoid the use of “we” and “our”.
* In the RoSI section, subsections could have been added to improve the readability.