# Security Investment - IoT Honeyspots
# Review of group 13 by group 3

**Summary**
The paper aims to investigate different risk strategies according to the problem owner and other actors involved in the security issue of IoT Honeyspots. It defines different metrics that can be retrieved from the dataset such as top-10000 malicious devices per ISP over time and total requests per country over time that are supposed to show the extent of exposure to attacks to the ISP. Furthermore it mentions attack and risk strategies of involved actors.
The paper concludes that the costs of incidents are trivial to ISPs since they cannot be held liable for the consequences of attacks and that NaWas is a cost effective solution.

**Strengths**
- the section of the problem owner is well described

**Major issues**
- chapter 3 mentioned 4 attack strategies but only 2 are listed. Isn't the way the strategy is carried out a part of the strategy (operation), rather than a new strategy?
- The metric evaluation section is missing a written evaluation and interpretation of the graphs. Therefore it is not clear what can be concluded from those numbers.
- lack of references and citation style; makes it hard to trust the liability of the statements and to conduct further reading to the reader.

**Minor issues**
- The introduction is not clear regarding the context of the paper. Try mention the topic of IoT Honeyspots/the security issue and the problem owner of the security issue in the beginning for better understanding. Putting the section of the problem owner to the beginning of the paper would have helped the reader to understand the overall context of the metrics without having to look at the previous assignment.
- Another actor could be a law enforcement agency that encourages regulations regarding the security of IoT devices. If this actor would be included you could have calculated the ROSI for their security investments and the costs of mitigating the incidents.
- Missing a conclusion/summary of the findings. It would be interesting to mention that the ISPs should become liable for creating insecure devices to protect major incidents in the future and that this is a major issue which needs to be tackled.