Summary

This assignment revolves around Internet of Things security issues. The security issues of IoT will have impact on various actors, from users to ISPs. Having said that, the problem owner of the IoT security issue are the vendors because vendors may see strong incentives to develop a solution for the problem. The security metrics reveal probability of breach of different vendors. Famous companies have better breach probability than the not so famous ones. The strategies for companies with breach probability < 14% are risk mitigation, and those with breach probability > 14% are risk acceptance.

Another actors that can influence the security measures are consumers, government, and ISPs. Actors may influence the issue along with their purchasing decision; the consumers will probably decide against purchasing equipment with high breach probability. The government may also affect the security issue by implementing relevant policy or legislation. Lastly, the IPSs have the capability to filter botnets' traffic by, for example, extracting its signature.

There are four types of strategies that can be implemented by the problem owners as well as the other actors. The strategies will be described one by one and the implementation of every actor that utilizes the strategy will also be explained.

First, the risk acceptance strategy. The vendors utilizes this strategy regarding the default password vulnerabilities. Even though the vulnerability is high but the impact is considered to be low, hence the risk is accepted and not mitigated. Consumers also may choose this strategy when they deal with the IoT credentials issue. Lastly, the government is applying this strategy because the fact that the technology is still new and no policies or regulations in place yet.

Second, the risk mitigation strategy. Vendors may implement this strategy by getting rid of default credentials and require their users to create a unique password instead. The governments may also utilize this strategy by implementing certain regulation or policy for the vendors. The customers may also implement this strategy but only in the situation where they have deep understanding regarding this security issue. Last, the IPSs are capable in mitigating this issue by blocking malicious traffic from infected IoT devices.

Third, is the risk transfer strategy. The vendors can also be said to have transferred the risk of default credentials of their IoT devices through terms and conditions. Consumers can also transfer the risk to a third party vendor who is capable in mitigating such risk. The ISPs are not always capable of transferring risks. There is some ISPs however, such as Corero, that is capable of transferring this security risk by filtering malicious traffic.

The last strategy is risk avoidance. It is stated that there are currently no actor implementing such strategy.

For the ROSI calculation, this group based their calculation on two different strategy: vulnerable device replacement strategy and lawsuit cost analysis. These ROSI calculations are supplied with formulas and sample of its applications.

Strength:

1. Clear and quite comprehensive analysis, especially regarding question number two: the security metric.
2. The visualization of the security metrics really helpful to understand the message that the writer is trying to convey.

3. Broad descriptions of actors strategies, although one or two addition can help make this section better.
4. The ROSI calculation seems impressive. The team has identified range of factors and equipped the calculation with reasonable assumptions. The ROSI calculation also backed with convincing reference.
5. The overall quality of the writing is nice and easy to read.

Major Issues:

1. Section 6, last paragraph: government have been accepting risk -> this claim is not supported by any information or reference.
2. Section 6.3, third paragraph: consumer hires third party that can help to prevent the risk. What kind of third party? Without any example it is difficult to argue that this is a sound risk transfer strategy. If the third party is a kind of cyber security consultant, this could be a risk mitigation strategy instead.
3. How about customers implementing risk avoidance strategy? For example, cautious type of users may choose not to adopt the IoT technology altogether because of the security issues rumour that spread through the news.

Minor Issues:

1. Paging would be nice.
2. Page 6, bottom left: the explanation for lawsuit cost analysis ROSI is a bit messy.