Deliverable 5 Risk Report

Daniel Benesh - CMPT 371 - Team 3

In this risk report, we will note parts of our project that are incomplete, features that could be improved, testing that still needs to be done for full coverage and other issues that would improve the overall quality of the Beap Engine web app.

1. Password Recovery: Probability 6, Impact 6

   At present we have not implemented a feature where the user can retrieve their current password if forgotten. We currently do not have an easy solution for the user to recover it. The risk involved is that users may lose access to their data which is not ideal. There are privacy concerns regarding users' email addresses. Our specifications did not specify a way to solve this problem. For future changes, the implementation would have to be fully fleshed out considering personal information as a primary concern since the files related to the user are health related. Some questions that could be asked of the stakeholder: Can the site store the users email and/or other contact information? Should there be 2-factor authentication should a password reset be implemented? What are the legal consequences should a data breach occur?

   Going forward, password recovery would be a valuable feature to implement and to mitigate the risk concerns, the details of the feature would need to be fully fleshed out to encompass all the issues related to the feature.

2. Big Data (Load Testing): Probability 4, Impact 8, Recurring

   During meetings with the stakeholder it was stated that no more than 10 users would be using the web app concurrently. If the project expands and many more users begin to use the web app, more testing would be needed to ensure that the data being processed would be able to handle many requests concurrently. The risk in not being able to handle many requests concurrently is that the system could completely crash, processed files may produce errors, may corrupt data and/or other unforeseeable issues. This could bring the app to a screeching halt. In passed risk reports we considered using an open source analytics engine for large-scale data processing. We looked at options such as Hadoop or Spark. These are open source frameworks that would be a solution to this problem.

3. File Types: Probability 5, Impact 9

   The current file types that our system accepts are xml and csv for Apple watch and Fitbit respectively. We have not extensively tested for different types of xml and csv files that are not the format that the system expects when processing the data. There are many different types of files that have the same extensions. It would be nearly impossible to test all files that have the same file extensions. The risk involved is that the system could exhibit undesired behaviour when trying to process those files. When the system processes those files the system may crash or cause other errors in the system. Going forward more testing of xml and csv files that are not explicitly Apple Watch or Fitbit would be beneficial to ensure that no unintended behaviour materialises.

4. SQL injections: Probability 3, Impact 10

   We have not tested the possibility of an sql injection when uploading files to the database. With our current knowledge of computer security we have not devised a plan to test how the system handles such an attack. The risk of this attack would have personal health data leaked to nefarious external actors. Testing could be improved to ensure that this type of attack is not possible, or at least unlikely. Greater security on this type of attack or others would be a valuable feature that is beyond the scope of our team.

5. Website on Mobile Devices: Probability 8, Impact 4

   The website does not render properly on mobile devices. Although usable, it was not built with mobile devices in mind. The risk associated with a messy UX on mobile is that it makes the web app less accessible. If the only experience a user has is with the mobile device webpage, the user's impressions will be negative, and may not want to use the Beap Engine services. Some consideration to this issue should be dealt with in the future if the intent is to be able to transfer files directly from a users mobile device to the web app.

6. Backend Code Coverage: Probability 3; Impact 6

   In this project we have been working with an already built backend. We have tested most of what we needed to to get the app up and running. There could be greater code coverage on the backend. The risk of not having the backend fully tested is that there may be bugs that have not yet materialised. The bugs could cause errors in storing/processing data. With a larger focus on code coverage for this part of our repository would allow us to be more confident that the code works as expected.

7. R repository Code Coverage: Probability 3; Impact 6

   Same as with the backend, we did not write the R-repository and do not know the extent to which it was tested. There could be bugs lurking in this repository. The risk involved is that the R repository would produce inaccurate data sets for the user. This would be detrimental to the entire purpose of the App. Going forward, the R repository could be tested more thoroughly to ensure that we can be confident that the results of processing the activity data is correct.

8. Next Developers: Probability 2, Impact 7

   In the future there could be new developers working on the project. There is a risk that they may not understand the codebase, which would make it difficult to pick up where we left off.. We have mitigated this risk by creating a lot of documentation, flow diagrams, architecture designs, function stubs, testing matrices and other such documentation that will help the next developers understand the codebase. We hope to have left this project in good standing.

9. Personal Health Data: Probability 4, Impact 4

   The stakeholder has informed us that health data can be deleted at the request of users. This would involve deleting data from the database. There is a risk that those who perform system maintenance would have trouble removing personal user information. We have mitigated this risk by documenting how to access the backend of the system. This should be sufficient in allowing information to be deleted on request.

10. Post Project Support: Probability 5, Impact 8

    After handing off this piece of software, there will be site maintenance that may occur. Software in the project may become deprecated. The site would need to have new packages installed to the ever changing software environments. This could result in the site not functioning as expected. To mitigate this risk we have left our names on the site so that if maintenance is needed, our team would be able to assist the stakeholder in updating the software used on the website.