Risks

There can be many risks involved in developing a mobile application with so many apps available in the market. Some of those risks include a too many features, time constraints, limited knowledge of coding and risk of security breaches through our application.

Fitness apps were downloaded 400 million times in 2021 (Curry 2022). With many options available on the app store, our application must have features which users need or want that cannot be provided by other fitness apps. One of the risks our project holds is that users feel the goal of this app can be reached through other fitness apps and does not use our application. Hence, our features such as child friendly workout plans, notification systems with encouraging quotes and the social aspects in sharing to online forums and individual social media accounts, hopes to satisfy the wants and needs of the users. However, another risk we run into while adding these features is that there is a possibility that our application is overrun with features that there are too many features. Since an application should try to focus on fulfilling a specific goal of the user, if our application has too many inbuilt features, not only could it make the user experience more difficult and unappealing, but we may also have difficulty developing a highly functional application within the given time constraints.

Although it is important to become familiar with the chosen software to develop the app and learn the programming language, with the time constraints in place it could be a risk that we do not become familiar enough with the software in due time. We have started using Kotlin to start developing the application and have come across a hurdle that there has been an update to the language for carrying out the tasks we would like. Hence, extra time is now required to relearn the language and methods to achieve our goals with the interface and functions of our application.

Data protection, security and privacy are all now prevalent issues in the media regarding technology and smart phones. Security issues are also another risk that our project could run into. He, Chan and Guizani (2015) explain that mobile application developers should ensure their app abides by security governance and does not access unnecessary information. It is important to encrypt any private data that is stored both locally and on remote servers, as well as providing extra security add-ons so that their application can fight against a security breach in the event the user’s mobile phone comes under vicious malware attack (He, Chan and Guizani 2015). In order to combat against any malware or security breaches, our application must have all the necessary features and certificates, but this can also challenge the time constraints if our mobile application proves that it is not secure enough.

Although there is a possibility of hardware risks and hardware crashes, since most of the work will be saved and backed up to collaboration cloud services such as GitHub, it appears that any hardware risks can be decreased. Also, since more than one person will be working on the development of the application and many in the team are currently android users, there will be many ways to work around any individual hardware problems that may arise.

Reference:

Curry, D 2022, ‘Fitness app revenue and usage statistics (2022)’, *Business of apps*, viewed 7 Feb 2022, <https://www.businessofapps.com/data/fitness-app-market/>

He, D, Chan, S & Guizani, M 2015, ‘Mobile application security: Malware threats and defenses’, *IEEE wireless communications*, vol. 22, no. 1, pp. 138 – 144.