IRM reflection

In the Collaborative discussion 1, I have a deeper understanding between qualitative and quantitative assessment: When will have a specific criteria or target to test, we need a qualitative assessment. A qualitative assessment helps us to have a more accurate result to a specific risk for testing; or to prove what I am guessing about a security risk is correct; A good qualitative assessment can lead to a quantitative assessment. A quantitative assessment can provide us a pool of samples, which is based on the qualitative assessment I have done during the initial stage. We can figure out the probability of the specific problem when it is wide spreading to our network.

I also have learnt human factor to reduce the cyber security risk in our organisation. As human is one of the biggest sources to create any potential threat. Also, not everyone in the organisation is computing literate. Education and training to the users in the organisation has the following benefits:

- Training staffs can help users to build the skills of identifying and avoid any security threat, which helps to reduce the security risk due to the human errors.

- Monitoring and review the risks by members of the risk management team, can help us to target the cause of the risk and minimise its impact. Owner and user monitoring should be progressed on a frequent and regular basis, to prevent any possible threat. (Spears & Barki, 2010)

In the discussion, I have discovered that it is impossible to find every single potential security threat. It may not be discovered if we only have a very less sample, such as in a qualitative assessment; or the impact of the threat is minimised after there are large quantity of users.

To maximise the effectiveness of assessment, I have learnt from IEEE (2000) that both qualitative and quantitative risk management to be used at the same time: We can create a super dataset through the Rick balancing Profiles, quantitative assessment, combining with the Defect Detection and Prevention, to measure the risk with its quantitative methodology.

In the design document, I was responsible to the business challenge. I have learnt there is no bespoke COT system for my own specific business, we need to make sure the COT is compatible with our existing business model, also can meet the necessary security standards.

Although open-source software becomes popular nowadays, with a lot of benefits. For example, bugs are easy to be discovered and can be fixed by any developer. But on the other hand, hackers will also discover these vulnerabilities, which can be found on public, such as the National Vulnerability Database. Therefore, for security, I don’t recommend rely on open-source software (Cypress Data Defence, 2020).

Also, I have discovered any inexperienced developer, like students, are not the best person to take part the development. They may lack of necessary resources to learn the skills and knowledge, how to develop a secure and robust software. Inexperienced developer will increase the risk of security threat. It can be more bugs and vulnerabilities to be created, the patching, security fixes and updating of the code may be inadequate or too slow. Also, there is a risk for inexperienced developer to response immediately once the software has occurred any issue, from operational to its own security. For example, when a hacker has broken into the system.

In the collaborative learning discussion 2, I have learnt and understood different causes behind the risk. For example, an improper systems security engineering not only will create the security issues, but will also affect the stakeholder’s relationship, product reliability and overall efficiency.

Besides the security aspects, for example, functions, and boundaries and system interfaces, I also have learnt other factors, such as design constraints, performance measures, also the tracking of system security requirements, we need to understand how to satisfy stakeholders security demands, should be included for consideration in the planning phrase. Also, other factors such as, the viewpoints, context, domain should also be defined when during the designing phrase of the system (Rumana, 2021).

I also need to explain the mitigations of the causes that I have mentioned in the discussion. I have learnt we need an experienced development team for the project; more factors need to be included on planning, tracing should be included while the development; I will also explain to stakeholders if some functions are eliminated due to the security requirement, more than one solution can be deployed on different SDLC stages, with discussion and approval from the stakeholders if any similar project in the real world (Ross, 2018).

On the risk assessment report, I was responsible to predict the risk and their possible causes. I have suggested the use of open-source software, inexperienced developers, and vulnerabilities of the COTs will be the possible causes of the risk. I found that the open source will be used by hackers and attack the weak point of the system easily; COTs may not be compatible with our current system, which may cause security hole; inexperienced developers, as I have discussed earlier, may destroy the system indirectly because of bad coding and cannot response to the bugs immediately and deploy the patches.

References:

1. Sutton, D. (2014). Information Risk Management. NBN International - Academic. https://online.vitalsource.com/books/9781780172675 [Assessed 16th August 2021].

2. M. S. Feather, S. L. Cornford and T. W. Larson, "Combining the best attributes of qualitative and quantitative risk management tool support," Proceedings ASE 2000. Fifteenth IEEE International Conference on Automated Software Engineering, 2000, pp. 309-312, doi: 10.1109/ASE.2000.873685.

3. Cypress Data Defense (2020) 3 Open Source Security Risks and How to Address Them: What You Need to Know, Available from: https://cypressdatadefense.com/blog/open-source-security-risk/[Accessed: 31st August 2021].

4. The Virtual Learning Environment: Log in to the site (2021) . The Virtual Learning Environment: Log in to the site. Available at: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=273812. [Accessed 10 September 2021].

5. Ross, R., McEvilley, M. & Oren, J. (2016) Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, volume 1