Reflective Piece

https://mutegibeatrice.github.io/module3.html

Security and Risk Management module has given me both exciting and challenging experiences. All of which have gone towards the advancement of my knowledge and understanding in risk assessment approaches, Disaster Recovery plans, Business Continuity plans, Quantitative and Qualitative solutions and many more.

For instance, I gained insights into more threat models (such as: OCTAVE, PASTA, OpenFAIR, MITRE ATT&CK, CVSS, Trike) and how one can use 2 or more models to do a risk assessment, for example, how STRIDE and DREAD models are more effective when combined.

After we were provided a case study and we were to use it to create a Risk Identification report in groups, I was assigned to Group 1 and each one of us agreed to work on 2 separate risk assessment models so that later on we can discus between ourselves which one(s) is/are the best approach(es) to be applied on the case study's Risk Identification report.

During one of our group meetings, my group members (3) and I presented good arguments on the approaches we should apply, whereby as per my research:

- I presented OCTAVE-S model and even though it is designed for smaller organizations and flexible (both operations and IT teams can work together to address the security requirements of the organization), we did not choose it as an approach because it was very complex to deploy and only quantifies from a qualitative methodology (Violino, 2021).

Plus, I found it to be broad (due to existence of different types of OCTAVE models like OCTAVE FORTE, OCTAVE-S, etc), and also it was difficult to find a clear set of examples of reports on how it is to be implemented and structured on a report. Furthermore, the examples that I found on materials like (Binus, 2014), were too complex and broad, and would have definitely exceeded the 1000-word limit on our report.

- After also looking at MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) framework, I viewed that it would have played a crucial role in targeting, analysing and mitigating attacks, evaluating risks and attack attribution. This is because it is a globally-accessible knowledge base of cyber-attackers' tactics and techniques based on real-world observations (Anon, N.D.). However, it would have not been an effective solution if it would have been solely used.

After discussing all the models as a group, we came to a conclusion that OpenFAIR was a better solution to implement as a risk assessment approach. So as to keep the report to a 1000-word count limit, we could not go ahead and combine FAIR framework with other models like Attack trees or MITRE ATT&CK model. Even though using 2 or more frameworks is considered to be crucial and more effective in cyber risk analysis.

As from my research, I found out that MITRE ATT&CK model would have highly complimented FAIR framework. Therefore, if we would have paired the MITRE ATT&CK and FAIR together, we would have been able to prioritize risk management initiatives, provide clarity into the risk landscape as well as get answers on tactical questions (Dominick, 2020).

From the above, it is clear that it was challenging to design a 2000-word count, efficient and effective risk identification report that has all the necessary and highly beneficial information and solutions included.

Another challenging part was beating the project submission deadlines. We would do researches (my contributions have been described on my e-portfolio), send our findings to our group leader or the person tasked with compiling the report. We would then hold a group meeting so as to discuss and decide on what information is to be kept on the final main report and appendices. The compiler would then add the information on the final report thus resulting to a lot of workloads on him/her plus worrying on beating the deadline. This would have been mitigated by using google Docs application whereby one of the team members would create a document, then share the document between the team members while also giving them editing rights. This would result to each team member taking the initiative to work on the document in real time (after they have all decided on the information to be included on the final report). As a result, time-saving and reduction of workload would have been ensured.

Been a part of a team has not only advanced my soft skills (which are, communication, research, initiative, teamwork, time management, decision-making, problem-solving, respectfully sharing of thoughts), - but it has also allowed me to learn a lot from my teammates, and independent researches and learning. For instance, I got to have an insight into technologies like SaaS (Software as a Service) as a solution, vendor lock-in and its mitigations, etc.

All these skills gained have been beneficial in my personal growth and will also be building towards my profession in the cybersecurity domain. I have acquired the know-

hows of designing a risk assessment report using different approaches, although availability of more reports or real-life examples that demonstrate how models like OCTAVE, can be implemented and structured, would have been more helpful in learning and understanding it better.

In overall, the skills and knowledge that I acquired throughout this module has not only enabled me to perform a thorough risk analysis and mitigation on organisations, but also digitalize an organisation in to a risk-free or cyber-secured digital environment. Additionally, in the future I will be more open to airing out my thoughts and concerns about the group's mode of communication, beating deadlines and any other issues, - so that we find solutions and apply them. I will also motivate my team members and hold more meetings regularly (even sometimes with the lecturer for clarification) so as to contribute to the exchange of ideas and information between us while also improving the quality of our work.

References

Anon, N.D.. Mitre Attack. [Online] Available at: https://attack.mitre.org/ [Accessed 30 10 2022].

Binus, S., 2014. Implementation OCTAVE-S and ISO 27001 Controls in Risk Management Information Systems. ComTech, 5(2), pp. 685-693.

Dominick, S., 2020. Steps to Combine MITRE ATT&CK and FAIR to Focus Cyber Risk Management. [Online] Available at: https://www.fairinstitute.org/blog/3-steps-to-combine-mitre-attck-and-fair-to-focus-cyber-risk-

management#:~:text=The%20MITRE%20ATT%26CK%20Framework%20provides,cyber%20risk%20analysis%20is%20crucial. [Accessed 29 10 2022].

Violino, B., 2021. IT risk assessment frameworks realworld experience. [Online]
Available at: https://www.csoonline.com/article/2125140/it-risk-assessment-frameworks-real-world-experience.html
[Accessed 29 October 2022].