Security and Risk Management Module

Group 1 Meeting Minutes – Assignment 1

4th September 2022

Attendees: Jane Aldridge, Pearce Begley, Shailender Kudachi, Beatrice Mutegi

Enclosed are the actions and meeting notes, for the second meeting for the first team assignment:

- Assignment Overview (Jane)
    - The assignment is split into two parts, the first is a risk assessment of the current pampered pets organisation, and the second is a risk assessment of the digitalization process
    - Both parts include the selection of a risk methodology, the application of the risk methodology and justification for the selection, and a threat modelling exercise
    - There also needs to be a list of the proposed changes included

- Risk Methodology
    - **It was agreed by all team members that the Open FAIR risk methodology would be used for the case study**
    - The justification was that Open FAIR is a framework which can be applied to a small organisation such as pampered pets, which has 4 employees. NIST is another framework but is focused on the SDLC and software development. Pampered pets is too small an organisation to propose any internal software builds.
    - ISO is another framework but this is geared towards large organizations and the time to work through this approach couldn't be justified for Pampered pets.

- Octave can be used to supplement open FAIR, but open FAIR is a free product, whereas Octave is not

- **It was agreed by the group that the approach to the risk analysis should be qualitative and not quantitative**, because the data for a quantitative assessment does not exist

- It was agreed that the justification for the risk methodology, and the approach taken to threat modelling would be written up by Jane and circulated to the group for review (Action: Jane)

- **Threat Modelling**
  - It was agreed by the group that 8 threat modelling approaches would be used, the advantage of using multiple threat models was that a more thorough analysis could uncover additional threats. The resources and budget was also available to support this.
  - It was agreed that the following threat models would be used :
    - Stride and DREAD (Action: Shailesh)
    - PASTA (Action : Pearce)
    - CVSS (Action: Shailesh)
    - OCTAVE (Action: Beatrice)
    - Attack trees (Action: Pearce)
    - Mitre ATT&CK (Action: Beatrice)
    - OWASP (Action: Jane)
    - Open FAIR (Action: Jane)
  - Trike was not selected because it is focused more on supporting a security audit

- It was agreed that each team member would work on two threat models (see above)

Proposed changes to support digitalization

It was agreed by the team that everyone would complete the analysis to determine the changes required to support digitalization (Action: All)

Tasks for next Week

It was agreed that the following would be left to next week:

- Risk Mitigations
- Timeline and proposal
- Executive Summary

Next Meeting

The next meeting would be Sunday at 1 pm UK time