e-Portfolio Link- https://sahib015.github.io/e-portfolio/

During the last twelve weeks, I learnt about security and risk management. This module covered various aspects about the security and risks that affect the IT industry and possible wates of mitigating the risks.

In this module there were different activities that I was able to contribute in as part of a group and individually, such as the collaboration discussions, seminar activities, e-portfolio activities and being able to work in a group for the assessments.

The collaboration discussion topics were interesting and in particular I found the collaborative discission about CVSS more interesting than Industry 4.0. Prior to this module, I had only come across CVSS being a rating of a security threat. While contributing to the discussion forum, it broadened my knowledge regarding CVSS. While reading other colleagues posts in the forum, it made me understand that CVSS is not the only scoring method and additionally there are different factors to consider making it an unreliable source. The factors that make me feel that CVSS is an unreliable scoring criterion are (1) the CVSS formula, (2) there is no evidence that the formula is robust, (3) the CVSS formula is not transparent about how the formula is derived and (4) the skill set of the individual scoring the vulnerability. With these factors in consideration, I think CVSS is more of a qualitative risk method instead of a quantitative risk method.

Working in a group for the assessment was an interesting experience as this allowed me to work with other colleagues in the course. While working on the assessments with my colleagues in different backgrounds, help me learn from them and gain some of their knowledge. As I am currently not working in an organisation and in at my previous workplace, the organisation’s main focus is on physical security, and I had the basic understanding of the different security threats from my bachelor’s degree. I

learnt from them and would hopefully use what I learnt from them and during the course in the coming future.

The assessments of the module were challenging and interesting at the same time. With an organisation working to digitalise their business and begin the digitalisation process, there are different factors to consider which was outline as part of the requirements. I found the assessment an exciting challenge ahead as to evaluate the potential security risks of the organisation may have as a group while digitalising their business and what aspects to consider during the digitalisation, such as the importance of having business continuity and a disaster recovery plan for any possible disruptions that may occur.

One of the instances while working as a group, we had a challenge in creating the analytical hierarchal process (AHP) for the assessment. As for a consistent AHP, the consistency ratio must be less than 0.1 however we were getting a consistency ratio of greater than 0.1. At this stage, we were confused whether we got the calculations wrong and after further research, according to (Business Performance, 2019), we realised that it is okay to have the consistency ratio greater than 0.1. This meant that there could be inconsistency in the supply chain making room for areas to improve the consistency of a supply chain.

As mentioned earlier, there were several tasks within this module that had individual activities. There was an individual activity regarding Monte Carlo simulation that had some exercises in excel. During this activity, there was some confusion I had on a particular question that was slightly misleading and contacted my tutor for assistance. With the discussion I had with the tutor, I was able to understand the scenario and clear the confusion I had, I was able to complete the activity. This can be found in my e-portfolio Module 03 section Risk Modelling Activities.

In general, this module was very interesting and educative for me. At my previous workplace before I left the organisation, the organisation had a ransomware attack, and I was unable to mitigate this from happening due to the lack of knowledge and expertise despite working with another colleague managing the IT infrastructure of the organisation. At the time of the ransomware attack, there was no disaster recovery plan nor business continuity in place for such incidents apart from a data back-up that was not recent as it was about 2 months old. This module made me understand the importance of business continuity and disaster recovery plan for any organisation. As a result, the organisation had lost its data of about 2 months and the time it took to recover from the ransomware attack with a poor recovery point objective (RPO) and recovery time objective (RTO).

Reflecting back to the time the organisation had the ransomware attack after this module, I have learnt that it is important to perform regular checks on policies, ensuring all standard regulations are in place. Had I known how important business continuity and disaster recovery plan is, continuous risk analysis and performing security system checks, I would have been in a position to advise the head of the IT department on the implementation process of a disaster recovery plan. After this module, it has not only educated me on the security risks and ways to manage them but also the importance to educate others to create awareness on the potential security risks they may have as an organisation or as an individual. By creating awareness, this educates others who are unaware of the risks and how they could potentially reduce the security risks that they may encounter in the future in the digital world.