E-Portfolio link

https://jhines2022.github.io/eportfolio/module%202.html

Reflective Review

This reflective review will briefly cover the units during my learning experience on this module, but units 7&8 will delve deeper due to the impact that quantitative risk analysis teachings had on me personally and how I wish to move forward. It will then reflect on my experience as a member of the development team projects and my individual contributions to the team activities before finally concluding.

Units 1&2 Covering Security and risk management definitions, concepts, processes, qualitative and quantitative assessments.

The PDCA Mandate of ISMS helped me to understand how chapters 4-10 of 27001 fit into the 4 phases. Before this unit, I had not heard of Open FAIR but soon realized how beneficial it would become when discussing standards.

Units 3&4 Threat Modelling Techniques.

This taught me about Attack trees, CVSS and the STRIDE & DREAD models. At the time of learning these, I had not been aware of the limitations around CVSS and that it is a qualitative scoring system. As the module went on, It dawned on me how our risk impact and vulnerability tables are based on subjective data and that we should be looking at implementing quantitative, probabilistic models as soon as possible.

Units 5&6 Standards, GDPR & PCI-DSS.

The GDPR case study helped me understand that although the UK has left the EU, legislation had remained for the subcategory of Personal data protection (Section 2(1)(c)(ii)), even after the 2019 amendment to this subcategory (Legislation, 2022) and that GDPR is still just as effective, post brexit.

Units 7&8 Quantitative Risk Modelling

These units impacted me the most, changed my thinking and cemented my future goals.

I discovered that a key benefit of learning quantitative risk analysis is the ability to accurately assess and measure the risks associated with various security threats. Often, risk assessment in cyber tends to be a subjective process, relying on the experience and expertise of security professionals to make judgments about the likelihood and impact of potential threats. However, with the advent of advanced analytical tools such as Monte Carlo simulation, Bayes theorem, and TOPSIS, this module has shown me that it is possible to conduct more rigorous and objective risk analysis.

For example, by using Monte Carlo simulation, we can simulate a wide range of potential security scenarios and assess the likelihood of different outcomes. I now have the confidence to present my analysis in a clear and concise manner, using data and statistics to support my findings. This new skill set will be extremely beneficial for my career, my inquisitive mind to discover the topic more and to prepare for a quantitative future in Cyber as the threat landscape continues to evolve and become more complex.

Units 9,10&11 Business Continuity and Disaster Recovery

Learning about cloud disaster recovery strategies, how costs vary depending on RTO and RPO requirements based on system level critically that then pre-define whether an active-active solution is required or an alternative, has been extremely interesting. This topic helped me to grasp the technical knowledge that will help me communicate more effectively with my colleagues from different departments when working on projects together. Learning about the 6 stages of digital transformation and Blue-Green deployments was very helpful.

Unit 12 What will be the most Influential trend in SRM in the next 5 years.

Considering the unit content and the second half of the module being focused around quantitative modeling, it seemed only natural to create a PowerPoint presentation on the topic of artificial intelligence for cyber risk quantification as a potential future trend in security risk management. This led to interesting discussions about AI data poisoning and attack vectors.

My experience as a member of the development team project & my individual contributions to the team activities.

Key challenges of team work is being able to coordinate and collaborate with other individuals who may have different goals, motivation and work ethic. This had been difficult in the beginning, especially when team members work at different paces and time zones. But later on, when the team members shared the same vision and drive as one another, then the results were extraordinary, enjoyable, motivating and bonding.

Working in teams during this module has been a good learning experience and I have managed to take away some very important points for future team projects.

One of the most significant and enjoyable benefits that I experienced was having the ability to leverage the unique skills, knowledge, and expertise of each motivated team member. By working together, team members combined their talents and produced high-level work.

Working in a team can be a fun and rewarding experience. Collaborating and working together provided an opportunity for our team members to form strong bonds that created a positive and supportive work environment, while there will always be challenges to working in a team, the benefits and excitement of working together can make it a very rewarding and fulfilling experience.

Conclude

The units in this module have developed me in many ways by either exposing me to new things and opening my mind to explore the topics in more depth or changing my way of thinking for how to approach these topics within my work environment.

I found several of the topics to be tough, such as, building a monte carlo simulation specifically on cyber risk with the correct variables and deciding how to present the data, if i needed to run more scenarios and simulations or how to ensure I had the correct data for the analysis that we required. I often discovered that I could approach the topic from a different aspect by observing simulations of other industries and how they approached subjective and objective data when creating a monte carlo simulation. It was this learning approach and experience which has inspired me to look deeper in cyber risk quantification for risk management and to incorporate probabilistic modelling into my daily work.

(Word count 990)

Reference

Legislation (2022) The data protection, privacy and electronic communications Regulations 2019. Available from: https://www.legislation.gov.uk/uksi/2019/419/regulation/2 [Accessed on 10 December 2022].