Security and Risk Management March 2023: Individual Reflection

Through participating in the Security and Risk Management March 2023 module, I have gained an in-depth knowledge of various concepts, approaches and standards related to security and risk management.

Unit 1 introduced the fundamental concepts of risk management. Stoneburner et al. (2008) defined risk as the net negative impact resulting from vulnerability exercises; risk management involves identifying, assessing, and mitigating risks to an acceptable level; this unit provided me with an invaluable foundational knowledge base in risk management principles which I found valuable during this module.

Unit 2 introduced me to qualitative and quantitative approaches to risk evaluation Quantitative evaluation provides a clear view of damages and costs related to an evaluation subject; however, its application may be difficult and time-consuming (Dobrynin et al., 2018). While each has its advantages and disadvantages, my choice ultimately comes down to factors like available data, organisational context, stakeholder needs and user participation - specifically as it enhances the accuracy and relevancy of assessments.

Unit 3 introduced STRIDE and DREAD as popular approaches to evaluating security risks. STRIDE has a support tool and is the most used threat model (Hussain Erwin and Dunne 2011). DREAD, however, represents five rating criteria, including Damage Potential, Exploitability and Affected Users' Discoverability, which helps assess risks more effectively. These approaches helped me develop a framework to identify and evaluate threats.

In Unit 4, I learned how to assess and identify potential threats using threat modelling techniques. I realized how crucial it was to fully understand a system's components and vulnerabilities to manage risk effectively. The practical experience gained from learning techniques like attack trees, misuse scenarios and data flow charts were invaluable in threat modelling.

Unit 5 examined security and risk standards within industry and enterprise settings. I became acquainted with ISO 27000, PCI-DSS, NSIT and COBIT and ITIL frameworks - such as ISO 27000 for information security management; PCI-DSS provides security requirements for handling cardholder data, while NSIT emphasises practical information sharing practices among organisations conducting such data.

In our team's project for Unit 6, the Summary of Recommendations was assigned to me. This role enabled me to integrate the perspectives of my colleagues into coherent and unified suggestions. This task received positive feedback, which helped me refine my understanding of digitalization and risk assessment.

Unit 7 provided me with an in-depth knowledge of quantitative risk modelling (QRM). Through it, I gained a greater insight into its significance for providing numerical and probabilistic assessments of risks. We explored different approaches to QRM, such as Monte Carlo Simulations and Bayes theoretical models - techniques which enable organisations to make more informed decisions by quantifying risks and their potential impact.

Unit 8 expanded upon the concepts and applications of QRM, as well as real-world applications of it. For example, I learned how QRM could address problems like optimising security investments, evaluating control effectiveness, and prioritising risk mitigation and reduction efforts.

Unit 9 focused on Business Continuity (BC) and Disaster Recovery (DR) Planning. I learned the significance of creating these plans so organisations can continue essential operations during disruptions or recover quickly after disaster strikes. It was interesting that, up until the year 2000, disaster recovery plans were typically based on the 3-2-1 backup of data and documents (Nikolovski and Mitrevski, 2022).

Unit 10 explored practical applications and issues in disaster recovery implementations, with particular attention given to Disaster Recovery as a Service (DRaaS). I learned that DRaaS offers reduced costs, scalability, expertise, data privacy concerns, vendor reliability considerations and service level agreements in making informed decisions when adopting such solutions.

In Unit 11, my role was more challenging. I had to format, proofread, and conduct the final edit of our project. This task was completed in less than 24 hrs due to unforeseeable circumstances. Despite the stress, I could still focus and maintain my resolve to ensure our project was completed to a high standard which we sadly didn't. This experience taught me the importance of good time management, attention to detail, and the ability to work under pressure. These units were also a great learning experience regarding communication with others. It was important to me to accept criticism from my colleagues, even if it was sometimes harsh, which helped improve the quality of our output. Furthermore, was an important lesson in humility and the power of constructive criticism to promote personal growth and enhance group dynamics.

My contributions to these projects helped me grow in terms of my technical skills and improved my ability to work with others, accept criticism and perform well under pressure. In addition, my journey has helped me understand the importance of everyone's role in a team and the value of receiving feedback.

Moving to Unit 11. Technological, economic, and societal developments make security and risk management evolve astonishingly. Some key trends include AI-powered predictive analytics, automating response systems and advanced authentication methods, and applying economic principles like risk diversification, cost-benefit analysis, and incentive structures into security strategies. Although AI and automation can enhance security while decreasing risk, potential issues like privacy ethics misuse must be considered when making these decisions. Therefore, taking a holistic and balanced approach towards managing security is necessary.

Overall, the Security and Risk Management March 2023 module provided me with a thorough knowledge and skill base in various security and risk management aspects. Each unit added to my expertise in this field - from risk assessment approaches and standards, quantitative modelling techniques and future trends to artefacts like STRIDE/DREAD frameworks, ISO 27000 certification plans BC/DR plans; thus, giving me all the skills, I need for optimal security risk management protocols in the future.

References:

S. Hussain, H. Erwin and P. Dunne, "Threat modeling using formal methods: A new approach to develop secure web applications," *2011 7th International Conference on Emerging Technologies*, Islamabad, Pakistan, 2011, pp. 1-5, doi: 10.1109/ICET.2011.6048492.

Dobrynin, T. Radivilova, N. Maltseva and D. Ageyev, "Use of Approaches to the Methodology of Factor Analysis of Information Risks for the Quantitative Assessment of Information Risks Based on the Formation of Cause-And-Effect Links," *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2018, pp. 229-232, doi: 10.1109/INFOCOMMST.2018.8632022.

S. Nikolovski and P. Mitrevski, "On the Requirements for Successful Business Continuity in the Context of Disaster Recovery," *2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, Ohrid, North Macedonia, 2022, pp. 1-4, doi: 10.1109/ICEST55168.2022.9828701.