E-portfolio Link: https://prannoymulmi.github.io/e-portfolio/srm_main

Our daily life is full of uncertainties and complexities involving various risks at each step. For instance, driving is an everyday activity that people do to reach from point A to point B. This process has life-threatening risks, such as being in a severe accident which can occur at any point of driving. However, due to the benefit and convenience of driving, various rules and mitigations are implemented to reduce the apparent risk of accidents on the road. Similarly, different kinds of businesses also endure risks, which can happen in every step to gain maximal profit. Since risks are inevitable and are a natural process of achieving a goal, it is crucial to clearly identify and effectively manage them to avoid and reduce probable pitfalls. Security and Risk Management discusses the core concepts and methodologies of conducting risk management using different assessments, such as qualitative and quantitative analysis and methods to maintain business continuity.

In this module, our team analysed a brick-and-mortar company called 'Pampered Pets', wanting to expand its business through digitalisation and internationalisation. This analysis involved a critical evaluation of the company's infrastructure and its aims against potential risks which could create a possible setback to the corporation and its business continuity. In the process, two main types of risk management assessments were in focus: Qualitative analysis and Quantitative analysis.

Qualitative analysis allows businesses to quickly understand the risks by considering factors such as industry trends, expert recommendations on threats, and market condition risk based on subjective judgements rather than objective data. This analysis provides comprehensive quick decision-making methods, enhancing business adaptability. In the 'Pampered Pets' analysis, different methods such as threat modelling, CVSS (Scarfone et al. 2009), OWASP Top Ten, and risk matrices were used to conduct qualitative analysis assessments to identify the risk and recommended mitigations. However, this method is based on expert opinion, making it incomplete as many risk categorisations are subjective, often using high, medium, and low-risk ratings (Ramona, S.E., 2011). Despite this, qualitative assessments are still suggested, as this method provides a quick way to identify risks as SMEs do not have enough skilled workforce or financial support to carry out an in-depth assessment. The qualitative method offers a practical and easy way to perform a risk assessment required for the company (Armenia S et al., 2021).

Contrary to Qualitative analysis, quantitative analysis is based on research data, which enables more objective risk decisions (Hall, H., 2023). In the case of 'Pampered Pets', quantitative analysis was also carried out to analyse supply chain risks and loss due to cyber threats. In the assessment, the particular side of understanding and applying different quantitative assessments like Monte Carlo, Bayesian networks for supply chain risk analysis (Badurdeen, F et al., 2014), AHP-TOPSIS (Menon, R.R, V. Ravi, 2022), and Open-fair (Freund, J. and Jones, J., 2015) seemed intriguing and most attractive. Based on the learnings from different sessions, our primary goal was to research and implement different quantitative methods to identify the risk loss based on data.

For this assessment, the Monte Carlo simulation was used to predict the loss due to cyber threats and AHP-TOPSIS was chosen to rank the suppliers given in the identified risks. Monte Carlo simulation was chosen to assess the loss probability compared to other frameworks like Open Fair due to the simplicity of implementing and saving resources which

is usually an issue with SMEs like ‘Pampered Pets’. However, it must be noted that Monte Carlo depends on the statistical distribution chosen as the source of input variables. It could lead to false results if a non-matching probability distribution for the population is selected (Raychaudhuri, S., 2008). Monte Carlo is recommended for SMEs, but the downsides must be considered. Similarly, AHP-TOPSIS was chosen as multiple studies were already conducted with this method to select a supplier (Sabaghi M et al., 2015). All these methods were deemed suitable for the assessment by looking at the size and resources available, which still provided an objective result to identify risks for the company.

Furthermore, the assignments in unit 6 were applied with qualitative and unit 11 with quantitative assessment. Since using two methods simultaneously would scrutinise and mitigate various possible risks properly, both are precious in assessing risks and preparing the business. However, the qualitative method is considered mandatory even if the resources and the budgets are restricted since the business will be vulnerable to unidentified risks. Therefore, from a professional viewpoint, it is recommended that businesses carry out both methods but, with fewer resources, conduct only qualitative analysis.

Identifying the risks of ‘Pampered Pets’ by actively participating in brainstorming activities, discussion in the team, research, and documentation of the risks, has been my contribution to the team. As a software engineer currently in IT, the analytic mindset and programming skills have helped research and analyse our tasks more efficiently using programming languages such as Python. My understanding of digital domains and their risks, such as cyber threats and business continuity strategies, and analysing the different risks and impacts of specific domains added value to our projects. Our team then researched different quantitative risk assessment methods. Most of these methods were not easy to understand without knowledge of Statistics or Mathematics, which would also make the analysing process more efficient. Here, applying different quantitative analysis methods in the programming language Python made the process faster. Our analysis lies mainly on Monte Carlo for cyber risks and TOPSIS for supply chain risks, for which I wrote codes in Python to estimate the loss amount for the categorised risks. My other valuable contribution to the team was researching the different methods of disaster recovery for different requirements for RTO and RPO and implementing a strategy for ‘Pampered Pets’ to achieve a highly available system for business continuity of the system and do threat modelling and creating risk matrices for the qualitative analysis. While carrying out such technical processes, it was inevitable to work individually. However, we tried to ensure good communication and collaboration in the team by dividing the tasks and creating regular meetings to avoid misunderstandings.

Engaging in these assessments with other colleagues as a team has brought many advantages. Working in a diverse field, from IT to business, our team learned from each other’s experiences through collaborative decision-making and clear and concise communication with different areas of expertise and point of view. Handling and pitching essential and relevant ideas for obtaining precise results has been a challenge, but valuing and evaluating others’ opinions helped unblock many questions faster and more efficiently. We gained a deeper understanding of different security and risk management assessments and better coordination as a team.

References

Armenia, S., Angelini, M., Nonino, F., Palombi, G. and Schlitzer, M.F., 2021. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, p.113580.

Badurdeen, F., Shuaib, M., Wijekoon, K., Brown, A., Faulkner, W., Amundson, J., Jawahir, I.S., J. Goldsby, T., Iyengar, D. and Boden, B., 2014. Quantitative modeling and analysis of supply chain risks using Bayesian theory. Journal of Manufacturing Technology Management, 25(5), pp.631-654.

Freund, J. and Jones, J., 2015. Measuring and managing information risk. A FAIR Approach/J. Freund, J. Jones-Elsevier.

Hall, H. (2023) Evaluating risks using quantitative risk analysis. Project Risk Coach. Available from: https://projectriskcoach.com/evaluating-risks-using-quantitative-risk-analysis/ [Accessed: 28 May 2023].

Menon, R.R. and Ravi, V., 2022. Using AHP-TOPSIS methodologies in the selection of sustainable suppliers in an electronics supply chain. Cleaner Materials, 5, p.100130.

Ramona, S.E., 2011. Advantages and disadvantages of quantitative and qualitative information risk approaches. Chinese Business Review, 10(12).

Raychaudhuri, S., 2008, December. Introduction to monte carlo simulation. In 2008 Winter simulation conference (pp. 91-100). IEEE.

Scarfone, K. and Mell, P., 2009, October. An analysis of CVSS version 2 vulnerability scoring. In 2009 3rd International Symposium on Empirical Software Engineering and Measurement (pp. 516-525). IEEE.