**Individual Project: Executive Summary**

**Introduction**

The process of digitalisation, although comes with many risks both physically and digitally, is considered beneficial due to its potential sustainability. It also plays a crucial role in the development of the business as it allows the opportunity to “collaborate with the customers to match needs and attract new customers” (Isaksson et al, 2018:7). However, despite the many developmental advancements that can be achieved through digitalisation, transitioning to such a business model comes with a number of risks, as highlighted by Kovaite and Stankeviciene (2019). These include, but were not limited to: Technical risks, competence risks, behavioural risks, data security risks and financial risks. Digitalisation introduces a new risk to the business as it will be exposed to a range of severe and varied cyber threats that have the potential to cause financial, legal and reputational damage. The following executive summary will identify and quantify specific cyber threats that the business may face, analysing the severity of each threat, as well as the probability each threat has of occurring using a Monte Carlo simulation. The Monte Carlo Method (MCM) allows for an easy and efficient way to observe specific events and interactions which can be implemented at a large scale and repeated without limit. In turn, when assessing the risk, the probabilities of different scenarios can each be measured, and the outcomes are able to be predicted. The cyber attacks chosen for the simulation, in which the business leaves itself vulnerable to with the transition to digitalisation, have been chosen using historical data and case studies, the basis for the main threats selected are also explained.

**Basis for Assumptions**

1) Unauthorised attempts to access systems: This type of attack is very common. “In the year ending March 2022, the Office for National Statistics estimated that there were 1.6 million computer misuse offences, which included a 158% increase in unauthorised access to personal information” (Office for National Statistics 2023).

2) Insider threat: The subtle and dynamic nature of insider threats make detection extremely difficult. “The 2018 US State of Cybercrime Survey indicates that 25% of the cyber attacks are committed by insiders, and 30% of respondents indicate incidents caused by insider attacks are more costly or damaging than outsider attacks” (US State of Cybercrime 2018).

3) Phishing attack: By far the most common type of breach of attack. According to the Cyber Security Breaches Survey in the UK, 84% of businesses fell victim to at least one phishing attack (Cyber Security Breaches Survey 2024).

4) Malware attack: Also very common, with billions of attacks detected each year. According to the Kaspersky Security Network (KSN), 31.9% of computers were subjected to at least one malware-class web attack over the year (Kaspersky Security Bulletin 2016).

5) Denial of service attack: A prevalent threat in today’s networks as they are easy to launch, while defending against this attack is ‘disproportionately difficult’ (Loukas & Oke, 2010).

**Monte Carlo Simulation**

A screenshot of a computer

Description automatically generated

The frequency distributions in the table estimate how many events would probabilistically occur during a period of a year. Each event randomly generated by the frequency distributions is then matched by a severity function, which acts as the monetary impact of any individual threat. The three parameters represent the lowest, mean and maximum cost of the threat. For example, a phishing attack costs from a minimum of £750 to a maximum of £5000, with a most likely value of around £1300. After the data is generated using a Monte Carlo simulation, the total cyber risks can be shown with a histogram.

A graph with numbers and lines

Description automatically generated

The histogram shows that the total annual risk may range from £5,517.28 to £7.046.34 with a mean cost of £6,137.88.

**Summary of Results**

The data indicates that on average, a financial cost of £600 annually could be lost on cyber threats alone, discounting the other consequences of cyber attacks such as reputational damages and other legal costs that could occur as a result of that. As the majority of operational decisions will be implemented digitally, cyber attacks targeting the business will have disastrous effects on both the supply chain of the company and the quality of the products. In terms of probability, the data shows the estimated number of attacks annually for each type of threat (parameter 1). Such figures emphasise the risks faced as a consequence of digitalisation as the many other types of cyber threats were not included in this simulation as well as physical factors such as increase in labour and increased competition.

**Business Continuity/Disaster Recovery Strategy**

Based on the requirements outlined by the business, a disaster recovery (DR) strategy has been designed with the objective of ensuring that the demands of the company are met.

A diagram of a cloud server

Description automatically generated

As shown in the diagram, the requirements mean that an active-active solution must be implemented with two systems running simultaneously, making it a highly critical system. As a result of such strict DR requirements, this strategy would be very costly and require a high level of maintenance. One system can run on premise while the other can be on cloud, this will allow for versatility whilst also mitigating the potential of vendor lock-in as it will not be completely cloud-dependent. A traffic manager is installed with the purpose of monitoring both systems in case the other system fails, where it will be immediately switched to the working system without disrupting the user, as per the business DR requirements. Despite the issue of vendor lock-in, such a system is still hosted on cloud due to its flexible nature, allowing for a complex DR strategy with minimal disruption to the customers in the event that it must be invoked. This system also allows for an option to use a blue-green deployment strategy in which users can be switched over to one site to test code while the other site is held at the previous version, in case of errors with the new code. This DR strategy would be the optimal choice in terms of meeting the business requirements.

**Summary of Recommendation**

* General Data Protection Regulation (GDPR): It is required of every business, when processing data to adhere to the seven principles of GDPR: Lawfulness, fairness & transparency policy requirements, purpose limitation principle, data minimisation principle, accurate data storage, storage limitation principle, integrity and confidentiality principle and accountability principle. The business has a legal obligation to ensure that the GDPR standards are met, and it is crucial to mitigate certain cyber risks that could lead to incidents such as data breaches that could lead to the business being in breach of GDPR regulations. For example, regularly training members of staff regarding phishing attacks and other cyber threats can help to mitigate such risks.
* ISO 27001: An international standard for information security. It sets the standard for a diligent information security management system, with the aim of helping organisations and businesses to manage their information security covering individuals, processes and technology. This standard encourages businesses to run efficiently with cyber security in mind.

**Conclusion**

To conclude, with the transition to digitalisation, the business has a legal and ethical responsibility to ensure that the data of its customers is protected and GDPR standards are met. The rise in cyber crime has meant that the risk to switch to digitalisation has risen dramatically and measures must be put in place to ensure that the integrity of the business is maintained, and the supply chain and quality of the products are of a high quality.

References:

1. Alhajjar, E. and Bradley, T (2021). Survival analysis for windier threat: Detecting insider threat incidents using survival analysis techniques. Computational and mathematical organisation theory, pp.1-17.
2. Alhazmi, O.H. and Malaiya, Y. K (2013). Evaluating disaster recovery plans using the cloud. In 2013 proceedings annual reliability and maintainability symposium (rams) (pp. 1-6). IEEE.
3. Belvardi, G., Kiraly, A., Varga, T., Gyozsan, Z. and Abonyi, J (2012). Monte Carlo simulation based performance analysis of supply chains. International Journal of Managing Value and Supply Chains (IJMVSC), 3 (2), pp.1-15.
4. Crosweller, M. and Tschakert, P (2021). Disaster management and the need for a reinstated social contract of shared responsibility. International Journal of Disaster Risk Reduction, 63, p.102440.
5. Elg, M., Birch-Jensen, A., Gremyr, I., Martins, J. and Melin, U (2021). Digitalisation and quality management: problems and prospects. Production Planning & Control, 32 (12), pp. 990-1003.
6. Garnaeva, M. Sinitsyn, F., Namestmikov, Y., Makrushin, D. and Liskin, A (2016). Overall statistics for 2016. Blue book.
7. Gupta, B.B., Tewari, A., Jain, A.K. and Agrawal, D. P (2017). Fighting against phishing attacks: state of the art and future challenges. Neutral Computing and Applications, 28, pp. 3629-3654.
8. Isaksson, O., Hallstedt, S.I. and Ronnback, A. O (2018). Digitalisation, sustainability and servitisation: Consequences on product development capabilities in manufacturing firms. DS 91: Proceedings of NordDesign 2018, Linkoping, Sweden, 14th-17th August 2018.
9. Kovaite, K. and Stankeviciene, J (2019). Risks of digitalisation of business models. In proceedings of 6th International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering.
10. Kroese, D.P., Brereton, T., Taimre, T. and Botev, Z.I (2014). Why the Monte Carlo method is so important today. Wiley Interdisciplinary Reviews: Computational Statistics 6 (6), pp. 386-392.
11. Metropolis, N (1987). The beginning of the Monte Carlo method. Los Alamos Science, 15 (584), pp. 125-130.
12. Morrow, T., Lapiana, V., Faatz, D., Hueca, A. and Richmond, N (2019). Cloud security best practices derived from mission thread analysis.
13. Nurse, J.R.C., Creese, S. and are Roure, D (2017). Security risk assessment in internet of things systems, (pp. 1-9). Retrieved from https://www.cs.ox.ac.uk/files/9680/2017-itpro-ned\_author-final.pdf.
14. Ohm, M., Plate, H., Sykosch, A. and Meier, M (2020). Backstabber’s knife collection: A review of open source software supply chain attacks. In Detection of Intrusions and Malware, and Vulnerability Assessment: 17th International Conference, DIMVA 2020, Lisbon, Portugal, June 24-26, 2020, Proceedings 17 (pp.23-43). Springer International Publishing.
15. Olson, D. and Wu, D (2020). Enterprise Risk Management Models. 3rd Edition. Berlin: Springer Nature.
16. Opara-Martins, J., Sahandi, R. and Tian, F (2014). Critical review of vendor lock-in and it’s impact on adoption of cloud computing. In International conference on information society (i-Society 2014). (pp. 92-97) IEEE.
17. Prashar, A (2023). Towards digitalisation of quality management: conceptual framework and case study of auto-component manufacturer. The TQM Journal, 35 (8), pp.2436-2454.
18. Witkowski, M. and Wojaczek, A (2017). Cyber attacks and threats. T. Kosciuszki, (2), pp.184-194.