## Executive Summary

## 1. Introduction

This Executive Summary is a follow-up to the Risk Identification Report for Pampered Pets regarding the digitalisation of the business. It consists of two main parts:

1. The estimate of the potential risks that have an impact on the business for:
    a. Cyber risks
    b. Supply Chain risks
2. Business Continuity (BC)/Disaster Recovery (DR) Strategy.

## 2. General Assumptions

The following assumptions apply to both parts of this assessment:

- Pampered Pets business is UK based and will focus on customers within the UK/EU market.
- The data for the two risk modelling exercises is verifiable; however, several assumptions have been made in each part to make the data more comparable.

## 3. Cyber Risk Modelling

### 3.1 Methodology

Figure 1 presents detailed steps for Monte Carlo Simulation (MCS), used for cyber risk modelling. It has been successfully applied as a risk simulation model to Small-to-Medium Enterprises (SMEs) (Ncubukezi, 2020; Genest & Gamache, 2020). MCS technique uses “random sampling and statistical modelling to estimate mathematical functions and mimic the operations of [a] complex system” (Harrison, 2010).

Yasai's (MSIS, 2019) worksheet was used for MCS because it had most of the features required for the simulation. In addition, the MCS was carried out in Python with all the values from Table 1 using the formula from Santini et al. (2019), p. 3. Also, the probability exceedance curve (Figure 5) was calculated to find the probability of the loss of each threat and the total (for implementation) (Github, 2023a).

After identifying the cyber risks, extensive research was performed to find verifiable data for the MCS worksheet. Assumptions were made to retrieve or calculate the data (see Appendix A). After the distributions were determined for the frequency and the severity, the ‘Total Risk’ was calculated based on the formula of risk, frequency into severity. Top threats were identified, and the percentage of mitigations was applied, after which MCS was run again.

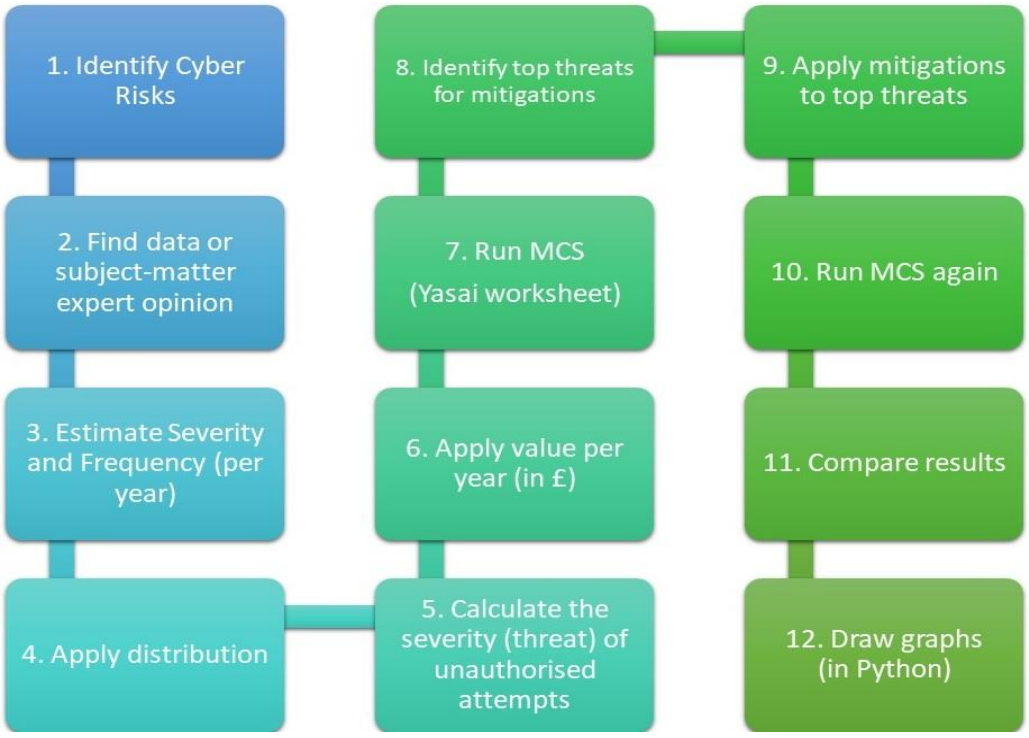


**Figure 1 – MCS Methodology**

### 3.2 Results

Table 1 contains the data obtained for the MCS research for each cyber risk identified. The data lists the number of occurrences per year (with up to 3 parameters), an estimated cost for each cyber risk (in £), the calculated risk for each cyber risk, and the 'Total Risk', which was 49082.27.

| # | Cyber risk | Frequency distribution | Param 1 (average nr. of events per year) | Param 2 | Param 3 | Frequency | Severity Distrribution | Param 1 (min. value £) | Param 2 (most likely) | Severity | Total (Frequency * Severity) | Nr of events after mitigation | Reduction in percentage | Total Risk after mitigation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | DDoS attack | Triagular | 34 | 76.66 | 111 | 61.98505521 | Exponential | 227,308 | | 1.1118E-06 | 6.89157E-05 | 55.7865 | 10% | 6.20241E-05 |
| 2 | DOS attack | Binomial | 3 | 0.05 | | 0 | Exponential | 22,430 | | 2.1988E-05 | 0 | 0 | 10% | 0 |
| 3 | Configuration errors | Triagular | 5 | 6 | 7 | 6.372361715 | Uniform | 1,000 | 10,000 | 6567.90533 | 41853.06845 | 5.73513 | 10% | 37667.76161 |
| 4 | Malware attack | Normal | 79.14 | 89 | | 0.238389701 | Uniform | 10,516 | 57,000 | 30323.6725 | 7228.85122 | 0.19071 | 20% | 5783.080976 |
| 5 | Phishing attack | Normal | 11 | 0.05 | | 60736.17896 | Exponential | 22,430 | | 5.8623E-06 | 0.356051141 | 54662.6 | 10% | 0.320446027 |
| 6 | Ransomware | Normal | 1.21 | 19.45 | | 1.61244E-14 | Exponential | 133,638 | | 2.1347E-07 | 3.44209E-21 | 4E-15 | 75% | 8.60522E-22 |
| 7 | Spam attack | Poisson | 5.22 | 4 | | 5 | Exponential | 22,430 | | 0.00010645 | 0.000532242 | 4.5 | 10% | 0.000479018 |
| 8 | Unauthorised access of files or networks | Poisson | 4 | | | 3 | Exponential | 22,430 | | 4.9239E-05 | 0.000147716 | 2.7 | 10% | 0.000132945 |
| 9 | Insider Threat | Normal | 21 | 40 | | 0.000432701 | Exponential | 12,400 | | 4.1255E-07 | 1.78511E-10 | 0.00011 | 75% | 4.46277E-11 |
| 10 | Social engineering | Poisson | 203 | | | 223 | Exponential | 85,434 | | 6.4632E-06 | 0.001441302 | 44.6 | 80% | 0.00028826 |
| | | | | | | | | | | Total Risk | 49082.27791 | | | 43451.16399 |

**Table 1 – MCS Data**

The top cyber threats with the highest value of the individual 'total' severity are listed in Figure 2:

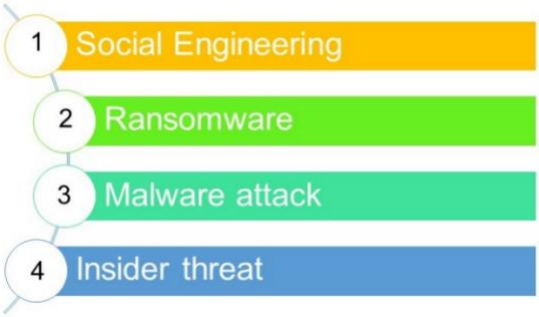


**Figure 2 – Top cyber threats**

The last two columns in Table 1 contain the data obtained after the mitigations were applied. The average mitigations for cyber threats were 10%, except for higher threats. The 'Total Risk' was reduced to 43451.16. Figures 3 and 4 present the Cyber Risks data before and after the mitigations were applied.

The results in the loss/exceedance curve (Figure 5) state that the loss of the Cyber Risk before the mitigation was 35% (£50,000), and it dropped to 20% (£20,000) after the mitigations. Also, the cost of £100,000 before the mitigation at 15% was reduced to 10% after the mitigations.

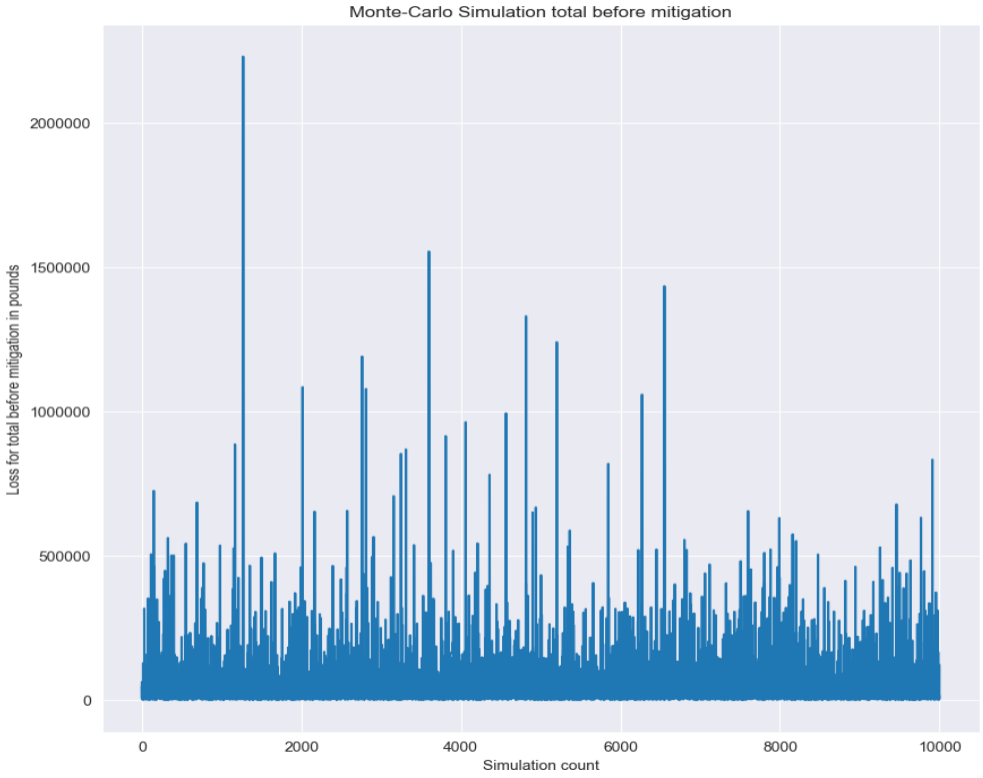


**Figure 3 – Cyber risks before mitigations**

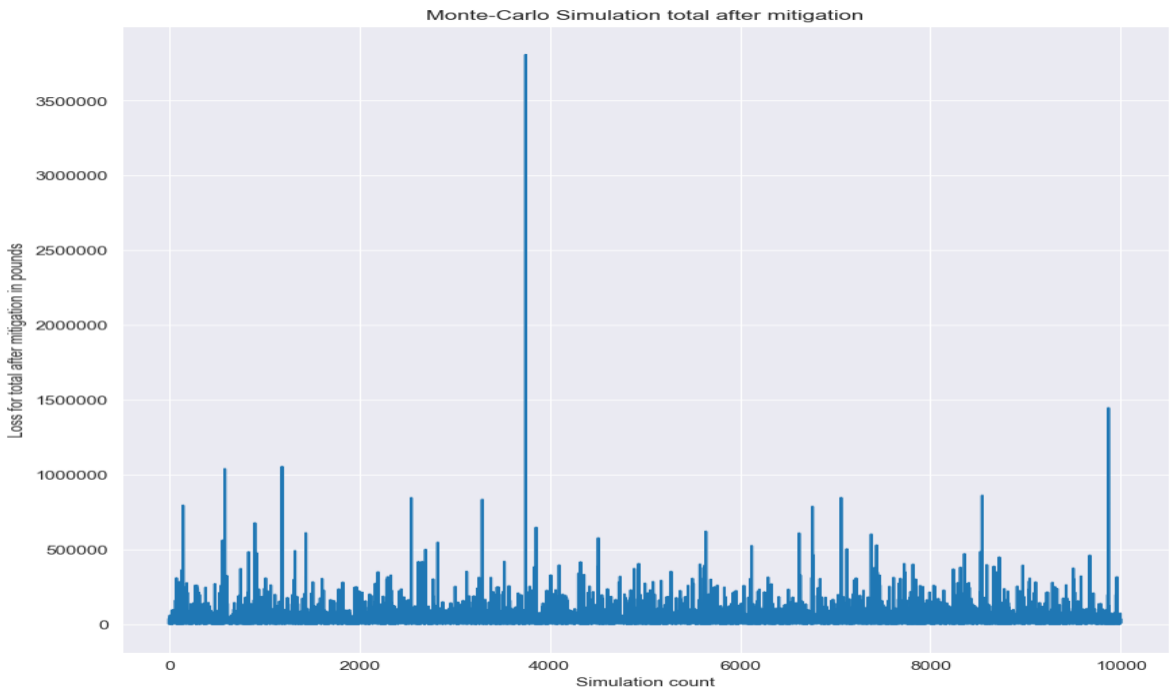


**Figure 4 – Cyber risks after mitigations**

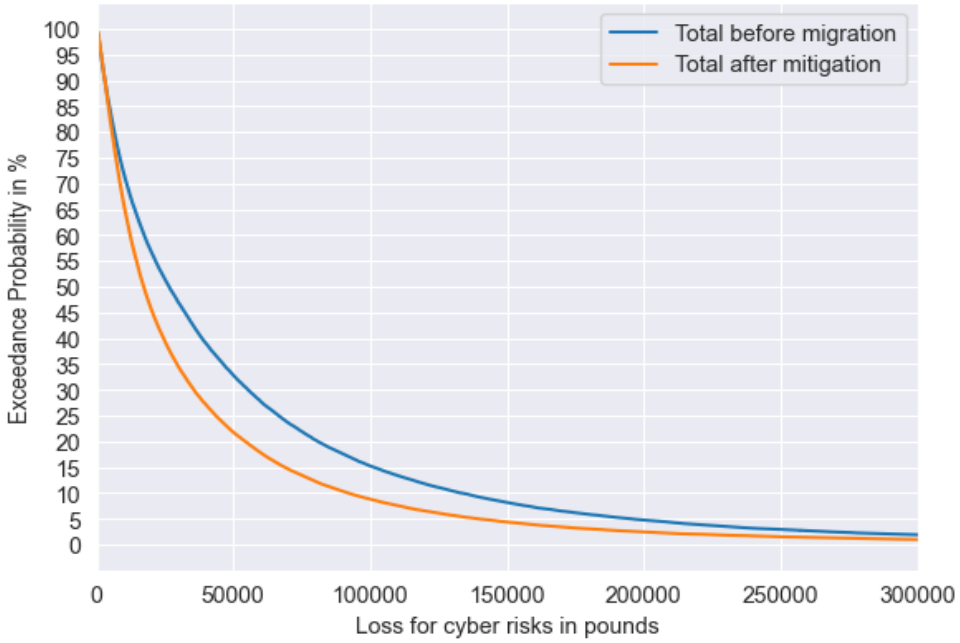


**Figure 5 – Loss-exceedance-curve**

### 3.3 Discussion

Applying mitigations (see Appendix B) to cyber threats would significantly reduce the 'Total Risk', and is highly recommended. However, further work is required to confirm the actual Total Risk reduction, as the risk reduction is currently just an assumption.

The comparison of the loss cost against mitigations is speculative and unknown until the mitigations are applied to the system (considering the end-system specs, cost, and locations).

MCS has proven helpful given the 'randomness' of the data it produced based on the parameters set. However, the results may vary with a larger, measurable data set with detailed analyses.

### 3.4 MCS Conclusions

MCS helped with identifying the top cyber risks, which were then mitigated. A set of technical, operational and additional controls suggested in Appendix B would reduce the severity of the identified risks. However, additional statistical and cost/benefit analysis might identify additional mitigations, further improving Pampered Pets business.

## 4. Supply Chain Risk Modelling

### 4.1 Methodology

To investigate the risks of the digitalisation of the supply chain, the Analytic Hierarchy Process with Technique for Order of Preference by Similarity to the Ideal Solution (AHP-TOPSIS) was used. Both are used to make data-driven decisions based on analyses.

The TOPSIS technique (see Figure 6) allows independent scoring of each alternative, giving users freedom (Sabaghi et al., 2015). Extensive research has been done to gather data for statistics based on the risks listed in Appendix C. A concise decision was made to shortlist 11 European countries (listed in Appendix D).

The very complex decision of picking a supplier according to different risk criteria was solved using the AHP-TOPSIS method, one of the Multiple Criteria Decision-Making (MCDM) processes (Menon, RR et al., 2022). The reasons for choosing the AHP-TOPSIS method were as follows:

- Multiple studies applied TOPSIS to select a supplier, similar to choosing the warehouse location, making it a good choice for this report (Sabaghi M et al., 2015).
- Finding the least risky location requires applying multiple criteria using the MCDM process.
- AHP was selected to complement the decision-making process with TOPSIS as it combines both quantitative and qualitative aspects in the decision method, which

helps the analysis to find the best possible answer rather than a correct solution (Longaray, A.A. et al., 2015).

- The subjectivity of AHP weights is kept in check with the consistency ratio, which allows a 10% error, allowing an efficient quantitative analysis (Longaray et al., 2015).

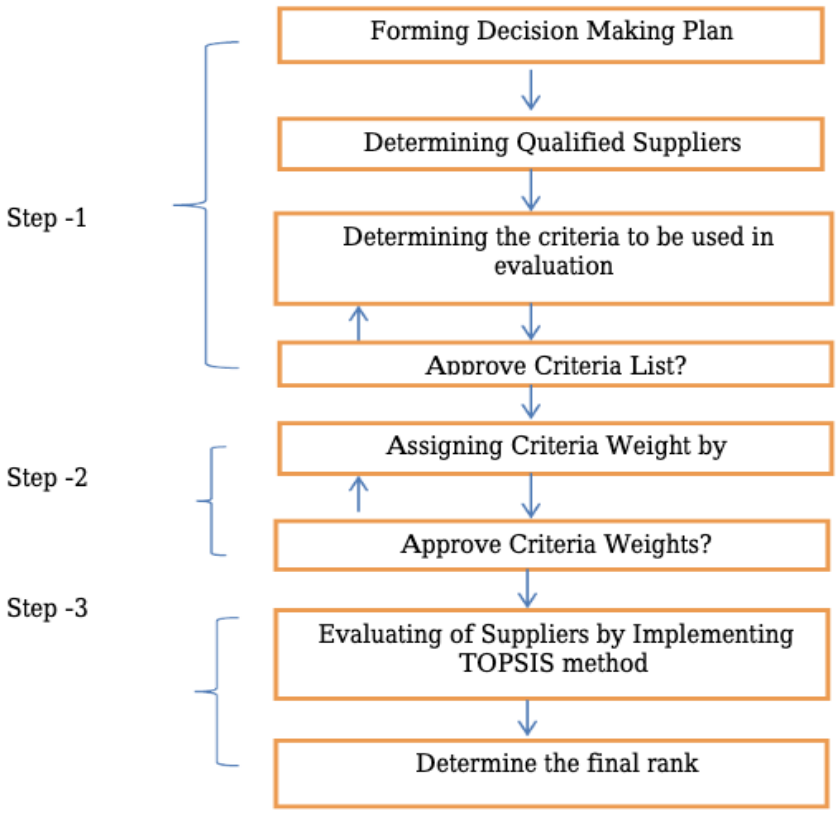


**Figure 6 TOPSIS methodology for warehouse selection (Vimal, J et al., 2012)**

AHP Assumptions:

- Subjective values for the AHP pair-wise matrices for weight calculation.
- Due to limited data availability for all the countries, the warehouses are assumed to be within the EU/UK.

### 4.2 Results

Table 2 lists warehouse risks which can affect the Pampered Pets supply chain:

| Risks | Risk Associated Threats |
|---|---|
| Digital risks | Ransomware, malware infection and non-compliance with regulatory standards, IT infrastructure failures, data breaches (Hudnurkar et al. 2017) |
| Political Instability | Government policies change, and the suppliers face additional customs and red tape (Olson & Desheng, 2020) |
| Natural Disaster | • Unexpected disasters like floods, earthquakes, tornados affect the supply chain (Olson & Desheng, 2020)<br>• Diseases, epidemics and pandemic, i.e., H1N1, Covid-19 (Chowdhury et al., 2021) |
| Manufacturing facility breakdown | • Facility breakdown<br>• Worker's strike (Hudnurkar et al., 2017) |
| Product risks | • Unavailability of raw materials.<br>• Unacceptable product quality (Hudnurkar et al., 2017) |

**Table 2 - Supply Chain Risks**

#### 4.2.1 AHP Results

The weight for each criterion used in the TOPSIS analysis was calculated (for results, see Appendix E). For Python implementation, see GitHub (2023b). Table 3 shows the results of the weights for each criterion based on the defined risks.

| Criteria | Weight |
|---|---|
| Digital Preparedness | 0.503 |
| Logistic Index | 0.249 |
| Political Stability | 0.114 |
| Natural Disasters | 0.084 |
| Labor Strikes | 0.05 |
| Consistency Ratio | 0.044 |

**Table 3: Weights**

#### 4.2.2 AHP Data Selection

The data sources listed in Appendix B were selected because they fit the purpose of this analysis. The data correlates to the risks identified in Table 2 regarding the best possible location ranking.

**TOPSIS Results**

AHP-TOPSIS (Table 4) shows the ranking of the warehouse locations with the best alternative using the closeness coefficient calculated in the method. It followed the AHP-TOPSIS methods shown in Appendix E.

| Candidate | Score |
|---|---|
| Germany | 0.871467 |
| Spain | 0.738019 |
| UK | 0.717268 |
| Ireland | 0.716363 |
| Netherlands | 0.708795 |
| Poland | 0.686061 |
| Belgium | 0.667067 |
| Hungary | 0.660432 |
| France | 0.523559 |
| Portugal | 0.510447 |
| Bulgaria | 0.460087 |

**Table 4: Best alternatives for warehouse locations**

### 4.3 Discussion & Conclusions

Pampered Pets is committed to growing its trade and has decided to add an internal supply chain with some automated warehouses internationally as part of the business plan. The location of selecting automated warehouses in different regions may impact the decision due to risks mentioned in Table 2.

The annual cost of global supply chain disruption is over $184M (Placek, 2022), which could affect Pampered Pets. Therefore, conducting a quantitative analysis of different countries where automated warehouses are located with the least risk possible is crucial.

For this reason, the quantitative assessment for the best alternative regions to setup their supply chains were performed for Pampered Pets, as shown in Table 4.

The AHP-TOPSIS method was helpful in selecting the best possible automated warehouse location for Pampered Pets and is recommended to use every time such a selection process is needed.

## 5. Business Continuity/Disaster Recovery

### 5.1 System Requirements


**Figure 7 – DRO / RPO**

As per Figure 7, the Recovery Point Objective (RPO) is 1-minute meaning; the system should be able to recover any data up to 1 minute before the disaster occurs. The Recovery Time Objective (RTO) is 1-minute, meaning after the disaster occurs, the system should be able to recover within the 1-minute timespan.

Also, a high availability (24/7/365) and near to real-time recovery strategy is required, as the system should not lose any data within one minute, and Pampered Pets can only tolerate 1 minute of downtime.

### 5.2 DR Strategies

Several different DR strategies are compared in Table 5, followed by assumptions made before DR plan steps were established.

| Features | Active/Passive | Active/Active | Disaster Recovery as a Service (DRaaS) |
|---|---|---|---|
| Cost | Low-high depending key strategies selected | High due to replication of site in another region | Low-Medium due to less complexity and manpower |
| RPO/RTO | Hours-Minutes | Minutes-Seconds | Hours-Seconds configurable as per requirements |
| Switch time to DR site | Hours-Minutes | Minutes-Seconds | Minutes-Seconds Automatic |
| Manpower | Fewer manpower needed due to lesser complexity | More manpower needed due to greater complexity | Least manpower due service handling majority of the complexities |
| Testing and maintenance | Less effort and resources | More effort and resources | Supported by the provider |

**Table 5 – Comparison of DR Strategies**

Assumptions:

- Cloud technologies and services are used to host and run business-relevant infrastructures and software.
- There are no budget restrictions to the DR strategy.
- Sufficient manpower is available for DR implementation, i.e., Engineers, Managers, DPO for GDPR, legal team, finance.

DR plan:

- Multi-regional off-site backup.
- Encryption of all the data at rest.
- DR action plan, i.e., incident response and DR architecture.
- Restarting backup systems (servers).
- Staff members are updated about the DR Plan.
- Testing of backup and recovery procedures.
- Data integrity and retention validation (Warith, 2022).

**5.3 Recommendations:**

Research conducted by Rebah & Sta (2016) states that 73% of SMEs do not have a DR Plan because of the complexity, budget, and effort needed to implement them. Based on the DR system requirements and the above assumptions, DRaaS is recommended as it provides SMEs like Pampered Pets with quality DR models at a lower cost due to lesser complexity and increased flexibility (Rebah & Sta, 2016).

Compared to the traditional approaches of self-implementing DR, it offers additional benefits, as follows:

- Reduced costs by handing over operational responsibilities to third-party providers and support from the vendors.
- Configurable RTOs/RPOs without extensive effort.
- Possibilities to use other strategies, i.e., Active/Active without self-implementation.

It also provides possibilities to implement an Active/Active (Warm) strategy, ensuring an RTO and RPO in under 1 minute, as seen in Figure 8.

This Active/Active method will ensure BC and deter damage that may disrupt the business as data centres are far apart, and if a disaster occurs in one region, the other region remains unaffected (AWS, 2023).

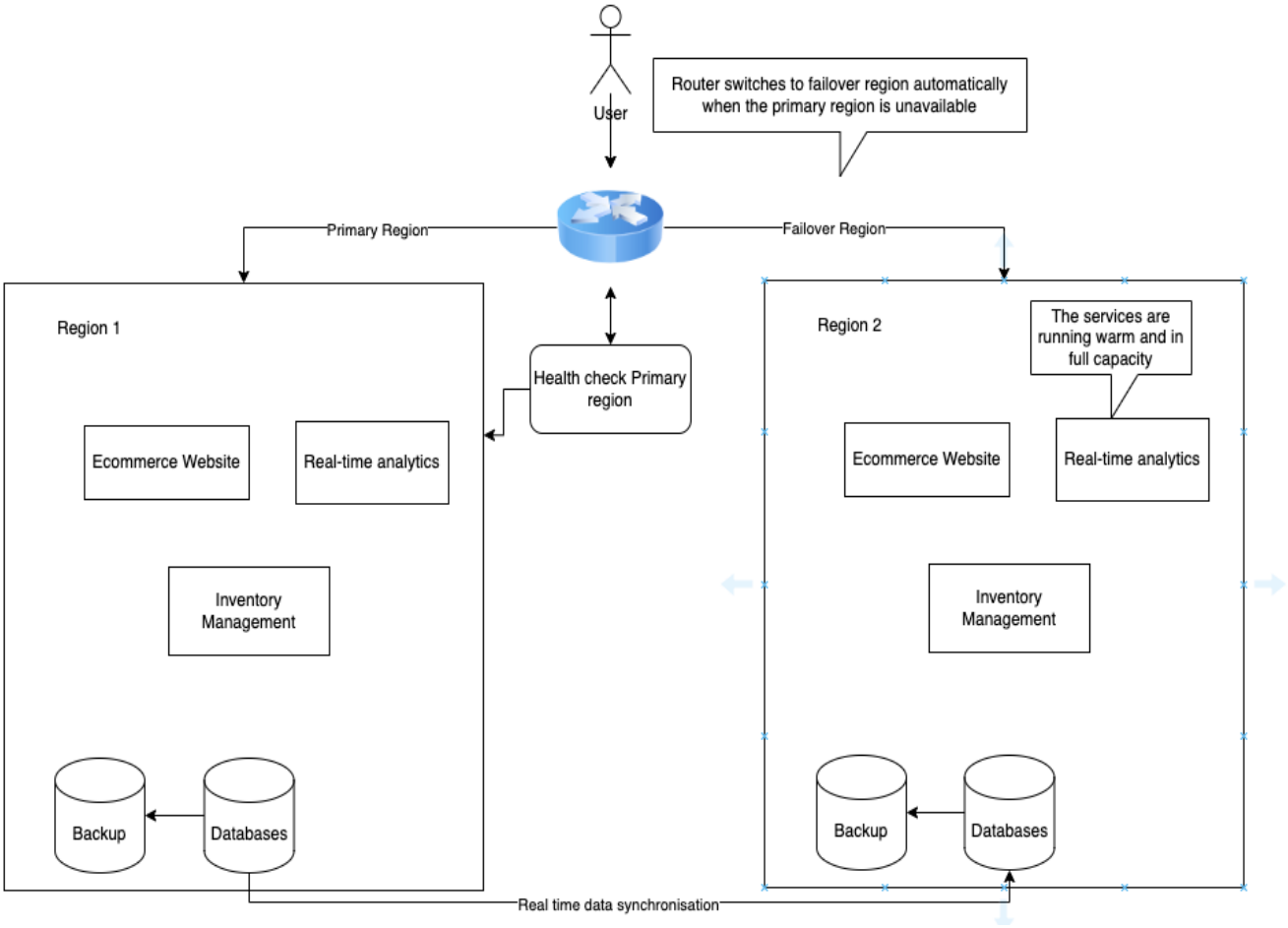


**Figure 8: Active/Active Disaster Recovery**

### 5.4 Platform Evaluation

In addition to choosing the DR strategy, two different Cloud vendors for hosting were compared for Pampered Pets (see Table 6) and two suitable DRaaS providers (see Table 7), which can impact BC.

| AWS | Azure |
|---|---|
| Mature services are available as existing from long time | Fewer services are available as compared to AWS |
| The essential services offered by AWS like storage and VM are more expensive than Azure | The essential services offered by Azure are affordable as compared to AWS |
| Difficult for first-time service users | Relatively easier as designed for business clients |
| Secured and reliable services with enhanced computational capacity | Easy to integrate and migrate from existing services |

**Table 6 – Cloud vendors**

| **Cloud4C** (Cloud4C, 2023) | **Druva** (Druva, 2023) |
|---|---|
| Both Active-Active and Active-Passive methods are available | Both Active-Active and Active-Passive methods are available |
| RPO and RTO less than 1 minute possible | RPO and RTO less than 1 minute possible |
| Multi-Cloud support, I.e., AWS, Azure, GCP, Oracle Cloud | DR Plan is only available in AWS and VMware environment |

**Table 7 - DRaaS Vendors**

### 5.5 Conclusions

Cloud computing allows clients to create a highly available, reliable and cost-effective way to run their business (Razavian et al., 2013). However, it also creates 'vendor lock-in' issues when the client wants to move away from the vendor. A multi-cloud approach is highly recommended to mitigate vendor lock-in issues (Pellegrini et al., 2017).

Therefore, based on Tables 6 and 7, hosting Pampered Pets in Azure cloud using Cloud4C as the DRaaS in AWS is preferred. This way, Azure could be utilised as it is easier for first-time users (see Table 6) for the primary region and use the DRaaS to host the DR in AWS with an Active/Active strategy.

Using the DRaaS, most of the complexity to the DRaaS provider would be offsite and would not have to dive deep into details with the AWS platform. In turn, this would require Pampered Pets to design their system using cross-platform services, i.e.,

Kubernetes, MySQL, MongoDB, and Docker, making the system more elastic to accommodate for multi-cloud, which would reduce the risk of vendor lock-in.

## 6. Security standards and mitigation for the business

The security standards for Pampered Pets are based on the CIA-triad (Confidentiality, Integrity and Availability). The following security standards are recommended in order of business priority:

1. General Data Protection Regulation (GDPR) serves as the most crucial standard in protecting the service user's rights and serves as a guide for the business to protect the personal information of the customer residing in the UK/EU.

2. Privacy policies and terms of service ensure that the data collected, stored, used and protected are clearly communicated with the service user.

3. Payment Card Industry Data Security Standards (PCI-DSS) ensure compliance with the payment methods.

4. Transport Layer Security/Secure Sockets Layer/Hypertext Transfer Protocol Secure (TLS, SSL, HTTPS) certificates provide service users with website safety verification and assurance.

5. Multi-Factor Authentication (MFA) implementation protects from unauthorised access.

The mitigations required to meet these standards revolve around implementing the above standards, strong passwords, timely updating and patching the system, employee training and awareness, incident response and management, and regular auditing (Arno, 2022).

## 7. Summary of Recommendations

The recommendations are based on several assumptions for each risk modelling exercise: the specifications, data, and limited selections of tools.

However, the selected methods were proven useful for the initial quantitative analysis and can help justify the direction Pampered Pets is going in terms of expanding its online presence and seamless BC with most minor business disruptions.

Without quantitative modelling and compliance with security standards, Pampered Pets might not take objective decisions in identified cyber, supply chain and DR risks and the impact these could have on the business. It will help make business decisions to ensure successful business growth and a robust online presence.

## References


Arno, H (2022). E-commerce Security 101: Essential Information For Web Store Owners. Available from: https://www.sana-commerce.com/blog/ecommerce-security-101/ [Accessed 19 May 2022].

Ashford, W (2016) Cyber attacks cost UK business more than £34bn a year, study shows. Available from: https://www.computerweekly.com/news/450300330/Cyber-attacks-cost-UK-business-more-than-34bn-a-year-study-shows [Accessed 15 May 2023].

AV-Test (2023) Mails per day - Mails with malicious attachments (12/05/2023). Available from: https://portal.av-atlas.org/spam [Accessed 12 May 2023].

Azure Network Security Team (2022) 2022 in review: DDoS attack trends and insights. Available from: https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/ [Accessed 10 May 2023].

AWS DR Whitepapers (2023) *Amazon*. Earthpledge Foundation. Available from: https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html [Accessed: 23 April 2023].

Chandra, A. (2020) Deep dive into analytical hierarchy process using Python, Medium. Available from: https://towardsdatascience.com/deep-dive-into-analytical-hierarchy-process-using-python-140385fabaa1 [Accessed 22 May 2023]

Chowdhury, P., Paul, S.K., Kaisar, S. and Moktadir, M.A. (2021) COVID-19 pandemic related supply chain studies: A systematic review. Transportation Research Part E: Logistics and Transportation Review, 148, p.102271.

Cloud4C: Fully managed DRaaS (2023) Advanced disaster recovery services on cloud. Available from: https://www.cloud4c.com/solutions/disaster-recovery-as-a-service [Accessed: 2 May 2023].

European Commission (2021) SME County Sheet 2021 - Romania. Available from: https://ec.europa.eu/docsroom/documents/46088/attachments/1/translations/en/renditions/native [Accessed 15 May 2023].

European Commission (2022) Flash Eurobarometer 496 (SMEs and Cybercrime). GESIS, Cologne. ZA7804 Data file Version 1.0.0, https://doi.org/10.4232/1.13950. [Accessed 14 May 2023].

Druva (2023) *DRaaS*. Available from: https://www.druva.com/use-cases/cloud-disaster-recovery [Accessed: 2 May 2023].

Genest, M.C. and Gamache, S. (2020) Prerequisites for the implementation of Industry 4.0 in manufacturing SMEs. Procedia Manufacturing, 51, pp.1215-1220.

GitHub (2023a) SRM - MCS Cyber Risks. Available from: https://github.com/prannoymulmi/Security-and-Risk-Management/blob/main/simulations/mcs_cyber_risks.ipynb [Accessed 21 May 2023]

GitHub (2023b) TOPSIS Implementation Available from: https://github.com/prannoymulmi/Security-and-Risk-Management/blob/main/simulations/topsis-implementation.ipynb [Accessed 21 May 2023]

GlobalEconomy.com (2021) Political stability - Country rankings. Available from: https://www.theglobaleconomy.com/rankings/wb_political_stability/ [Accessed 14 May 2023].

Home Office Science Advisory Council (2018) Understanding the costs of cyber crime - A report of key findings from the Costs of Cyber Crime Working Group. Research Report 96. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf [Accessed 15 May 2023].

Hudnurkar, M., Deshpande, S., Rathod, U. and Jakhar, S. (2017) Supply chain risk classification schemes: A literature review. Operations and Supply Chain Management: An International Journal, 10(4), pp.182-199.

Longaray, A.A., Gois, J.D.D.R. and da Silva Munhoz, P.R., (2015) Proposal for using AHP method to evaluate the quality of services provided by outsourced companies. Procedia Computer Science, 55, pp.715-724.

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.

MSIS Department of Rutgers Business School (2019) Yasai Simulation Add-in. Available from: http://www.yasai.rutgers.edu/index.html [Accessed 14 May 2023].

National Statistics (2022) Business population estimates for the UK and regions 2022: statistical release. Available at: https://www.gov.uk/government/statistics/business-population-estimates-2022/business-population-estimates-for-the-uk-and-regions-2022-statistical-release-html [Accessed: 15 May 2023].

Ncubukezi, T. (2020) A proposed: integration of the Monte Carlo model and the bayes network to propose cyber security risk assessment tool for small and medium enterprises in South Africa. International Journal of Computer Science and Information Security (IJCSIS), 18(3).

Netscout (2018) Cloud in the Crosshairs. In: NETSCOUT's 14th Annual Worldwide Infrastructure Security Report. Available from: https://www.netscout.com/report/ [Accessed 10 May 2023].

Office for National Statictis (2021) UK Dataset - Internet users. Available from: https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/datasets/internetusers [Accessed 12 May 2023].

Olson, D.L., Wu, D., Olson, D.L. and Wu, D. (2020) Data Envelopment Analysis in Enterprise Risk Management. Enterprise Risk Management Models.

Pellegrini, R., Rottmann, P. and Strieder, G. (2017) Preventing vendor lock-ins via an interoperable multi-cloud deployment approach. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 382-387). IEEE.

Placek, M. (2022) Supply chain disruptions - cost by country 2021, Statista. Available from: https://www.statista.com/statistics/1259125/cost-supply-chain-disruption-country/#:~:text=Supply%20chain%20disruptions%20are%20an,according%20to%20a%202021%20survey. [Accessed: 14 May 2023].

Proofpoint (2022) 2022 Cost of Insider Threats Global Report. [online] Proofpoint, Proofpoint, pp.6, 23. Available from: https://protectera.com.au/wp-content/uploads/2022/03/The-Cost-of-Insider-Threats-2022-Global-Report.pdf [Accessed 14 May 2023].

Razavian, S.M., Khani, H., Yazdani, N. and Ghassemi, F. (2013) An analysis of vendor lock-in problem in cloud storage. In ICCKE 2013 (pp. 331-335). IEEE.

Rebah, H.B. and Sta, H.B. (2016) Disaster recovery as a service: A disaster recovery plan in the cloud for SMEs. In 2016 Global Summit on Computer & Information Technology (GSCIT) (pp. 32-37). IEEE.

Sabaghi, M., Mascle, C. and Baptiste, P. (2015) Application of DOE-TOPSIS technique in decision-making problems. IFAC-PapersOnLine, 48(3), pp.773-777.

Santini, P., Gottardi, G., Baldi, M. and Chiaraluce, F. (2019) A data-driven approach to cyber risk assessment. Security and Communication Networks, 2019.

Seon (2023) Cybersecurity Countries. Available from: https://resources.cdn.seon.io/uploads/2023/04/Cybersecurity_countries-min.pdf [Accessed 14 May 2023].

Sophos (2022) The State of Ransomware 2022. In: A Sophos Whitepaper April 2022. Available from: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf [Accessed: 16 May 2023].

Statista (2023a) Annual number of malware attacks in selected countries in 2022 (in millions) Available at: https://www.statista.com/statistics/1085815/malware-attacks-by-country/ [Accessed 15 May 2023].

Statista (2023b) Average costs of all cyber-attacks in the United States and Europe from 2021 to 2022, by country. Available from:

https://www.statista.com/statistics/1327147/median-cost-attacks-in-cyber-security-united-states-europe/ [Accessed 14 May 2023].

Statista (2023c) Number of e-mail users worldwide from 2017 to 2025. Available from: https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/ [Accessed 12 May 2023].

Statista (2023d) Number of phishing attacks in Romania in 2020, by month. Available from: https://www.statista.com/statistics/1194551/romania-number-of-phishing-attacks-by-month/ [Accessed 16 May 2023].

Statista (2023e) Number of cyber attacks reported to the Italian CERT (Computer Emergency Response Team) from 2018 to 2021, by attack method. Available from: https://www.statista.com/statistics/649297/cyberattacks-distribution-share-by-method-in-italy-timeline/ [Accessed 18 May 2023].

Statista (2023f) Average costs of cyber insurance claims made by SMEs in North America from 2014 to 2018, by cause of loss. available from: https://www.statista.com/statistics/667597/cyber-insurance-claim-cost-north-america-by-cause-of-loss/ [Accessed 18 May 2023].

Vandaele, K. (2023) Strike map of Europe. Available from: https://www.etui.org/strikes-map [Accessed 14 May 2023].

Vimal, J., Chaturvedi, V. and Dubey, A.K. (2012) Application of TOPSIS method for supplier selection in manufacturing industry. *International Journal of Research in Engineering & Applied Sciences*, *2*(5), pp.25-35.

Wang, J., Neil, M. and Fenton, N. (2020) A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, *89*, p.101659.

Warith, N. (2022) Disaster Recovery Strategies To Keep Online Businesses Up And Running. Available from: https://www.forbes.com/sites/forbestechcouncil/2022/01/20/disaster-recovery-strategies-to-keep-online-businesses-up-and-running/?sh=5c6076992283 [Accessed 24 April 2023].

Wikipedia (2022) List of countries by natural disaster risk. Available from: https://en.wikipedia.org/wiki/List_of_countries_by_natural_disaster_risk [Accessed 14 May 2023].

Wise (2023) USD to GBP conversion. Available from: www.wise.com [Accessed 10 May 2023].

World Bank Group (2023) International LPI - Global Ranking 2023. Logistics performance Index (LPI). Available from:

https://resources.cdn.seon.io/uploads/2023/04/Cybersecurity_countries-min.pdf [Accessed 14 May 2023].

Worldometers.info (2023a) Germany Population. Available from: https://www.worldometers.info/world-population/germany-population/ [Accessed 10 May 2023].

Worldometers.info (2023b) UK Population Available from: https://www.worldometers.info/world-population/uk-population/ [Accessed 10 May 2023].

Yifat Perry, P.E. (2020) *Azure vs AWS pricing: Comparing apples to Apples*, *NetApp BlueXP*. Netapp. Available from: https://bluexp.netapp.com/blog/azure-vs-aws-pricing-comparing-apples-to-apples-azure-aws-cvo-blg [Accessed 1 May 2023].

## APPENDIX

## APPENDIX A – Data Source for MCS calculation

As mentioned in Section 3.1, all data entered in the MCS Table 1 is traceable. It can be sourced and validated. The calculations were made on a number of assumptions, where the data could not be directly found, which are also listed, unless in two examples, where subject matter opinion was applied (which is also clearly listed).

Due to space restrictions of this assignment, the table with the data source is attached in the Appendix. Data used in the MCS Table 1 in the document's main body is highlighted in yellow.

Note that the references used in this Appendix do not appear in the document's main body; however, full references have been added to the list of references in the Reference section.

| Cyber Risk | References, calculations and assumptions |
|---|---|
| [1] DDoS | References:<br>a) Azure Network Security Team (2022)<br>b) i) Netscout (2018)<br>ii) Worldometers.info (2023a)<br>iii) Worldometers.info (2023b)<br>iv) Wise (2023) |
| | Calculations:<br>a) i) Min. Number of attacks per day: 860; maximum number of attacks per day: 2,215 (globally)<br>ii) If UK IT infrastructure is 5% of the global IT infrastructure, then the number of DDoS attacks per year in the UK is between 34 and 111<br>b) ii) EMEA had 2.3 million DDoS attacks per year; the cost of DDoS in Germany was $351,995<br>iii) If the number of DDoS attacks per year in the EMEA, with the population of 2.1 billion people was 2.3 million, we can then assume that the number of DDoS attacks in the UK, with the population of 68,893,405 is 76.66 attacks per year<br>iv)If the cost of the DDoS attack in Germany, with a population of 84,544,972 is $351,995, we can then assume that the cos of the DDoS attack in the UK, with a population of 68,893,405 is $286,831; $286,831 converted to GBP is £227,308 |

| Cyber Risk | References, calculations and assumptions |
|---|---|
| | Assumptions:<br>a) UK internet infrastructure is 5% of the global internet infrastructure.<br>b) The number of DDoS attacks in the EMEA is proportional to the number of attacks in the UK (based on the EU vs. UK population)<br>c) The cost of DDoS attack in Germany is proportional to the cost of DDoS attack in the UK (based on the Germany vs. UK population)<br>d) The data from 2018 is somewhat still relevant in 2023 |
| [2] DOS | References:<br>a) European Commission (2022)<br>b) Statista (2023b)<br>c) Wise (2023) |
| | Calculations:<br>a) Q7 "Has your company experienced any of the following types of cybercrime in the last 12 months? (% EU27)" on p.32 represents the data for the SMEs: the number of DoS attacks is 3.<br>b) + c) The average cost of the cyber-attack in the UK in 2021/22 was $28,000; if converted to the USD (Wise, 2023), the sum is £22,430; the cost of the DOS attack could not be found, therefore it was assumed that this is a reliable number |
| | Assumptions:<br>a) The data available on the type of cybercrime per SME in the EU can be directly applicable to Pampered Pets<br>b) The cost of DOS attack in $ equals to the average cost of the cyber-attack in the UK, once converted to £<br>c) The cost of the DOS attack could not be found, therefore it was assumed that the average cost of a cyber-attack listed above is a reliable number |
| [3] Config. errors | This data was based on pure 'subject matter' opinions. Based on the team expertise, the average number of attacks was estimated to be 5, 6 and 7 attacks. The estimated cost of this cyber-attack was £1,000 and £10,000. All values were captured in the MCS table and included in the calculations.<br><br>Assumption: The number of configuration error attacks and an estimated values of this cyber-attack was based on subject matter opinions. |
| [4] Malware | References:<br>a) i) Statista (2023a)<br>ii) National Statistics (2022)<br>ii. Home Office Science Advisory Council (2018)<br>b) Ashford, W (2016) |
| | Calculations:<br>a) i. The number of malware attacks in the UK was 432.9 million in 2022; if this is applied to the number of small businesses (0-249 employees), which is 5.47 million, it can be estimated that the number of malware attacks per SME per year is 79.14.<br>ii. Between 2009 and 2014, the amount of malware attacks to the UK companies was 89; since this is an old data, and the number of malware attacks has risen since 2014, we can estimate that the average number of |

| Cyber Risk | References, calculations and assumptions |
|---|---|
| | malware attacks on UK companies (including the SMEs like Pampered Pets) has risen, and is now 89 per annum, rather than in 5-year span.<br>b) The average cost of the damage to IT infrastructure damaged by malware was £10,516 as of 2016; as of 2023 we can assume that this can now be a minimum cost to IT infrastructure rather than an average cost.<br>c) As per the Home Office Science Advisory Council (2018) reference above, the average cost of malware attack in the UK was £57,000 |
| | Assumptions:<br>a) The data for number of malware attacks applies to malware attacks in companies, not to a general population.<br>b) The average cost of damage to IT infrastructure from 2016 serves as a minimum cost of damage in 2023.<br>c) The old 5-year data (e.g., between 2009 and 2014) can count as an annual data (as of 2023)<br>d) The average cost of malware attack in 2023 is somewhat the same as in 2018 |
| [5] Phishing | References:<br>a) European Commission (2022)<br>b) i. Statista (2023d)<br>ii. European Commission (2021)<br>Iii. Wise (2023) |
| | Calculations:<br>a) Q7 "Has your company experienced any of the following types of cybercrime in the last 12 months? (% EU27)" on p.32 represents the data for the SMEs: the number of Phishing attacks is 11.<br>b) i. The number of phishing attacks in 2020 in Romania was 26,744.<br>ii. If Romania had 26,744 phishing attacks to 519,203 SMEs the number of phishing attacks on the 5.47 million SMEs in the UK can be estimated as 281,758 attacks per year for all UK SMEs – which is 19.45 attacks / year per SME.<br>c) i) The average cost of the cyber-attack in the UK in 2021/22 was $28,000; if converted to the USD (Wise, 2023), the sum is £22,430; the cost of the Phishing attack could not be found, therefore it was assumed that this is a reliable number |
| | Assumptions:<br>a) The data on the type of cybercrime per SME in the EU can be directly applicable to Pampered Pets<br>b) The number of SMEs in Romania is proportionate to the number of the SMEs in the UK<br>c) The number of phishing attacks applied to all SMEs in Romania is proportionate to the number of phishing attacks in the UK |
| [6] Ransomware | References:<br>a) Sophos (2022)<br>b) European Commission (2022)<br>c) Wise (2023) |
| | Calculations:<br>a) In the graph entitled "Percentage of Organizations Hit by Ransomware In the Last Year" on p. 12 of the report, it says that UK had 300 out of 5,600 |

| Cyber Risk | References, calculations and assumptions |
|---|---|
| | respondents, out of which 57% responded that they were hit by ransomware; if this is calculated per one organsiation, then we can divide 171 attacks by 300 organisations, which is 0.57 ransomware attacks per year per organisation<br>b) Q7 “Has your company experienced any of the following types of cybercrime in the last 12 months? (% EU27)” on p.32 represents the data for the SMEs: the number of Ransomware attacks is 4.<br>c) (refers to the same reference as above) In the graph entitled “Average Ransom Payments By Country” on p. 17 it says that the sum for the UK was $166.828, which is £133,638, when converted to GBP (Wise, 2023) |
| | Assumptions:<br>a) Since there is no information about the size of orgranisation, it is assumed that the size of organisations equally applies to the SMEs. |
| [7] Spam | References:<br>a) i. AV-Test (2023)<br>ii. Statista (2023c)<br>a. iii. Office for National Statistics (2021)<br>b. iv. National statistics (2022)<br>b) Wise (2023) |
| | Calculations:<br>a) i) The number of spam emails (12/05/2023) globally was 937 emails per day<br>ii) Since the number of internet users worldwide in 2021 was 4.147 billion, the above statement of 937 emails per day can be applied in principle<br>iii) The number of internet users in the UK in 2021 was 41 million, therefore the number of spam emails was 574 spam emails per day.. So each user experiences 0.106 spam email attacks per day, which is 38.95 spam email attacks per year<br>iv) If 41 million UK email users experience 38.95 spam emails per year per user, then we can expect that 5.5 SMEs will experience 5.22 spam email attacks per year per SME<br>b) i) The average cost of the cyber attack in the UK in 2021/22 was $28,000; if converted to the USD (Wise, 2023), the sum is £22,430; the cost of the Phishing attack could not be found, therefore it was assumed that this is a reliable number |
| | Assumptions:<br>a) The number of spam attacks per year globally correlates with the number of spam attacks per year per UK user<br>b) The number of SMEs using email corelates to the number of UK email users |
| [8] Unauthorised access of files or networks | References: a) European Commission (2022) |
| | a) Calculations: Q7 “Has your company experienced any of the following types of cybercrime in the last 12 months? (% EU27)” on p.32 represents the data for the SMEs: the number of Unauthorised access of files or networks attacks is 4. |
| | a) Assumptions: The data on the type of cybercrime per SME in the EU can be directly applicable to Pampered Pets |

| Cyber Risk | References, calculations and assumptions |
|---|---|
| [9] Insider threat | References: a) Proofpoint (2022)<br>b) Wise (2023) |
| | Calculations: Data is based on organisations in Europe, Middle East, Africa and Asia-Pacific:<br><br>a) "67 percent of companies are experiencing between 21 and more than 40 incidents per year" p.6.<br>b) Proofpoint classify insider threat as "employee or contractor negligence", "criminal and malicious insider" and "credential risk" - the cost of these annually are $15,378,635 [£12.4 million] - p.23.<br>c) Since the estimated cost was very high for this particular threat, the team decided to apply a more conservative number of £12,400 rather than £12,4M |
| | Assumptions:<br>a) It is assumed that the data on insider threat occurrence is directly applicable to Pampered Pets as an SME<br>b) The data on the cost of the insider threat has been conservatively reduced |
| [10] Social Engineering | References:<br>a) Statista (2023e)<br>b) Statista (2023f) |
| | Calculations: The number of social engineering attacks reported in Italy in 2021 is 203. The cost associated with the social engineering attack is 85,434 pounds. |
| | Assumptions: It is assumed that the number of attacks in Italy is proportionate to the number of attacks in the UK. |

## APPENDIX B – List of proposed mitigations

This list is in sync with the mitigations in the previous Assignment (SRM Assignment 1).

Note:

- Additional, cloud-specific, spec-specific, and region-specific mitigations might be required to align with the Pampered Pets business direction.
- A separate cost/benefit analysis is required to calculate the impact of each mitigation on the proposed Pampered Pets system.

| **Mitigations (in alphabetical order)** |
|---|
| Access controls with the least privilege |
| Anti-virus software |
| Authentication and authorisation controls to handle resources |
| Auto-scan file upload integrity check |
| Back/front of the house CCTV |
| Company cyber security policies: BYOD and removable storage devices |
| Continuous training |
| Data back-up and recovery plan |
| Data encryption, I.e., AES, RSA |
| Firewalls on hubs/devices |
| IDS/IPS |
| Implement DNSSec to protect DNS integrity |
| Incident response planning |
| Multi-Factor Authentication (MFA) |
| Protected entry |
| Secure payment systems (online and physical) |
| Separate Wi-Fi network (one for staff, one for customers) |
| Staff training (malware/spyware/phishing/ransomware and password management) |
| Strong password protection |
| System implementation of access logs, transaction logs, audit data and use SIEM to detect anomalies |
| Throttle requests from users |
| Updated/patched software |
| Use Ingress and Egress filtering |
| User WAF for application layers |
| Website should include CSRF tokens, and CSP headers |

## APPENDIX C – Data Sources for TOPSIS

Please note that the references used in this Appendix do not appear in the main body of the document. However, full references have been added to the list of references in the Reference section.

| Data | Description | Reference |
|---|---|---|
| Political stability | This index ranks how stable a country is politically | GlobalEconomy.com (2021) |
| Natural Disasters | The probability of natural disasters occurring in a country from 2011 to 2022 | Wikipedia (2022) |
| Workers strike in Europe | Average days not worked per 1000 employees in Europe | Vandaele, K. (2023) |
| Cyber security Index (Digital preparedness) | An Index which shows how good are country's digital infrastructure and preparedness against attacks | Seon (2023) |
| Logistic Index | This index is showing the logistic infrastructure in a country | World Bank Group (2023) |

## APPENDIX D – Countries used in AHP-TOPSIS

| # | Country |
|---|---|
| 1 | Germany |
| 2 | Poland |
| 3 | France |
| 4 | Belgium |
| 5 | UK |
| 6 | Portugal |
| 7 | Bulgaria |
| 8 | Netherlands |
| 9 | Spain |
| 10 | Ireland |
| 11 | Hungary |

## APPENDIX E

### I) AHP Weight Calculation

1. Pair-wise comparison of each criterion and sub-criteria to establish the weight of the supply chain parameters (see figure below).
2. Global summation of all these weights (weighted arithmetic sum) for each alternative and ordering them based on this weighted sum.
3. Calculate the consistency ratio, which should be less than 0.10, otherwise the weights are not balanced (Chandra, 2020).

| Features | Digital Prepardness | Natural Disaster | Labor Strikes | Political Stability | Logistic Index |
|---|---|---|---|---|---|
| Digital Prepardness | 1 | 6 | 8 | 4 | 3 |
| Natural Disaster | 1/6 | 1 | 3 | 1/2 | 1/4 |
| Labor Strikes | 1/8 | 1/3 | 1 | 1/2 | 1/4 |
| Political Stability | 1/4 | 2 | 2 | 1 | 1/3 |
| Logistic Index | 1/3 | 4 | 4 | 3 | 1 |

**Figure (Appendix E): n x n pairwise matrix with the importance of each criterion against each other**

**II) AHP-TOPSIS Calculations**

1. The values in the decision matrix are normalised to a value between 0 to 1 so that all the values are brought into a standard scale.
2. The weight calculated using the AHP method for each alternative is then multiplied to get a weighted rating.
3. The positive ideal solution and the negative ideal solution for each attribute are calculated. These values are either the maximum or the minimum value of each alternative.
4. The Euclidean distances of the PIS and NIS are calculated, which is used to calculate the closeness coefficient. This coefficient is used to rank the alternatives. The higher the value, the better it is.