Assignment 2:
Executive Summary – Pampered Pets

Authors: Amy Furnan, Steve Fisher, Antonios Kikidis & Stella Williams

Contents

Part I – Risks of Digital Transformation

1. Introduction

Risk assessment is essential to identify and mitigate potential disruptions to supply chains which according to Resilinc (2021), increased 67% in 2020 with single-source supplier issues a major factor. Companies that conduct risk assessments are better equipped to anticipate and mitigate disruptions to ensure supply chain resilience. Part I begins by reviewing historical and objective data, followed by simulations for both disaster and cyber risks assessment. Simulation results are then analysed, and recommendations for mitigation provided. Part II outlines a disaster recovery plan to ensure business continuity should a disaster occur.

2. Cyber Risks in the Supply Chain.

Recently, there has been an increase in supply chain attacks, necessitating more extensive and nuanced analyses (Fahimnia et al, 2015), hence it is crucial for Pampered Pets to understand the risks that apply to them. Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) is a decision-making technique which compares alternatives based on their relative proximity to both the ideal situation (no chance of an attack occurring) and the worst-case scenario (100% chance of an attack occurring). A summary of TOPSIS analysis, utilising data from the Mitre CAPEC database, is shown in Table 1. Using these risks, research provided insight into the average cost to a company of these attacks. For detail TOPSIS calculations see Appendix 1.

Attack Type	Likelihood	Severity	Skill Level	Performance Score	Probability of success	Potential Cost
Malicious Automated Software Update via Redirection	High	High	Low	0.84099717	4.2%	$21,041,666.66
Malicious Automated Software Update via Spoofing	High	High	Low	0.84099717	4.2%	$21,041,666.66
Malicious Logic Inserted into Product by Authorized Developer	Medium	High	Low	0.62110453	3.1%	$52,950,000.00
Development Alteration	Medium	High	Low	0.62110453	3.1%	$10,000,00.00
Malicious Logic Insertion into Product Software via Configuration Management Manipulation	Medium	High	Low	0.62110453	3.1%	$52,950,000.00
Malicious Logic Insertion into Product via Inclusion of Third-Party Component	Medium	High	Low	0.62110453	3.1%	$52,950,000.00
Design Alteration	Medium	High	Low	0.62110453	3.1%	$10,000,00.00
StarJacking	Medium	High	Low	0.62110453	3.1%	$1,000,000.00
Metadata Spoofing	Medium	High	Medium	0.544499026	2.7%	$1,000,000.00

3. Historical Data on Disaster Risk.

Data was classified into two categories: natural and man-made disasters and their potential impact analysed. Although several other factors can potentially affect supply chains, this study concentrated on these two factors, whilst making assumptions to facilitate comprehensive analysis, (See Appendix 2). Quality issues with supplied products were excluded from the discussion, as it was assumed that reputable businesses were chosen as suppliers, and such issues would therefore only arise in the event of a disaster or complete supplier failure.
Historical data of natural and man-made disasters was gathered for the 5 most agriculturally productive EU states in 2021 (World Bank Group, 2023). See Table 2.

Country	Agricultural Output Value (Billions)
France	$70.2
Italy	$60.5
Germany	$57.4
Spain	$53.6
Netherlands	$43.4

Table 2: Top 5 EU states by agricultural output.

Disaster data was extracted for these states from the EM-DAT database – a globally recognised database containing disaster records (Shen & Hwang, 2019) and spans five decades from 1973-2023.
Table 3 shows a summary of the percentage risk and potential cost of each disaster (Full calculations can be found in Appendix 2).

Disaster	Average Rate per 24 Months	Percentage chance of at least one disaster	Estimated cost per 24 Months
Geophysical	0.34	29%	$10,681,345.60
Hydrological	1.48	77%	$14,181,617.44
Climatological	0.43	35%	$1,064,210.00
Meteorological	2.22	89%	$12,767,400.40
Technological	2.35	90%	$1,499,796.32

Table 3: Disaster type, chance of occurrence and average cost.

4. Costing and Stock Data

To analyse the cost of ingredients and to simulate inventory risks, data was extracted from the European Commission Data-Modelling platform of resource economics[1] on the cost of the main ingredients of pet food produced by the 5 states over 20 years. Summaries are shown in Figures 1 & 2 (Full data analysis can be found in Appendix 3).

1. https://datam.jrc.ec.europa.eu/datam/mashup/EU_ESTIMATED_AGRICULTURAL_BALANCE_SHEETS/

Agricultural Total, Mean and Organic Production 2002-2022

Country		Mean production / Year (1000 T)	% Organic Area 2020	Mean Total Organic Production /Year (1000 T)
France	Cereals	65,274	9	6966
	Oil Seeds	6,284		
	Meat	5,839		
	Totals	77,397		
Germany	Cereals	46,020	10	5823
	Oil Seeds	4,756		
	Meat	7,456		
	Totals	58,233		
Spain	Cereals	20,573	10	2757
	Oil Seeds	908		
	Meat	6,092		
	Totals	27,574		
Italy	Cereals	17,084	17	3659
	Oil Seeds	1,015		
	Meat	3,425		
	Totals	21,524		
Netherlands	Cereals	1,717	4	184
	Oil Seeds	8		
	Meat	2,876		
	Totals	4,601		

Notes:
No data available for China in 2022

Figure 1: Agricultural Total, Mean and Organic Production 2002-2022.

Mean Agricultural commodity Producer Price Summary Data for 2018-2021

	Meat Price ($/T)				
	Bovine	Pig	Sheep	Poultry	Mean
France	4,447	1,609	6,937	3,669	**4,165**
Germany	3,802	1,807	3,956	5,595	**3,790**
Italy					
Netherlands					
Spain	2,646	1,352	3,226	1,248	**2,118**

	Oil Seed Price ($/T)						
	Rape	Soya	Sunflower	Poppy	Safflower	Sesame	Mean
France	453	429	508				**463**
Germany	467	450	424				**447**
Italy							
Netherlands	446			2,864			**1,655**
Spain	366	566	425		399		**439**

	Cereal price ($/T)				
	Barley	Maize	Sorghum	Wheat	Mean
France	192	204	205	210	**203**
Germany	210	194		211	**205**
Italy		224		246	**235**
Netherlands	215			222	**218**
Spain	204	235	204	238	**220**

All prices are 'producer price' obtained from the Food & Agricultural Organization of the United Nations (FAO)

Notes:
Blank cells indicate no data was available in the data set.
No oil seed data available for Spain in 2021

Figure 2: Mean Agricultural Commodity Producer Price Summary Data for 2018-2021.

5. Risk Analysis

Monte Carlo simulations (MCS) are employed due to their ability to accommodate multiple assumptions and leverage historical data where current data is lacking (Olson & Wu, 2010). The first simulation determines the likelihood of any potential risks occurring within the supply chain, while the second focusses on modelling and evaluating inventory stock levels.

5.1 Risk Simulation

An MCS was conducted to evaluate the likelihood of a risk and the average financial impact resulting from such an occurrence. A summary is shown in Table 4. The assumptions and calculations of the MCS are shown Appendix 3.

Chance of at least 1 risk occurring	98%
Expected Cost	$37,700,000.00
90% confidence interval	$7,800,000 - $83,100,000

Table 4: Summary of Risk & Cost

As there were large differences between disaster costs and cyber-attack costs, separate MCSs were undertaken with Table 5 and Table 6 providing a summary.

Chance of at least 1 cyber-attack occurring	24%
Expected Cost	$8,850,000.00
90% confidence interval	$200,000 - $36,300,000

Table 5: Results of Cyber Risk MCS

Chance of at least 1 disaster occurring	100%
Expected Cost	$33,900,000.00
90% confidence interval	$5,800,000 - $82,100,000

TABLE 6: Disaster Risk MCS

5.2 Stock Simulation

An MCS was performed to determine the best reorder point (RP) and reorder quantity (RQ) for the Pampered Pets inventory system. Seven possible scenarios of differing RP and RQ values were chosen, and the simulation ran for 1000 random observations of each. The RP and RQ of each scenario are shown in Table 7 and a summary of the MCS is shown in Table 8. Full calculations are detailed in Appendix 3.

Scenario	**Reorder point (RP)**	**Reorder quantity (RQ)**
1	500	600
2	500	700
3	500	800
4	500	1000
5	600	700
6	600	1000
7	700	2000

Table 7: RP & RQ values for each scenario.

Output Name	**Scenario**	**Observations**	**Mean**
Any stockouts?	1	1000	0.297
Any stockouts?	2	1000	0.269
Any stockouts?	**3**	**1000**	**0.196**
Any stockouts?	4	1000	0.027
Any stockouts?	5	1000	0.000
Any stockouts?	6	1000	0.000
Any stockouts?	7	1000	0.000
Total profit	1	1000	237634.390
Total profit	2	1000	238600.809
Total profit	**3**	**1000**	**239120.091**
Total profit	4	1000	237931.141
Total profit	5	1000	236271.453
Total profit	6	1000	237659.803
Total profit	7	1000	229211.553

Table 8: Results of MCS of each scenario.

Scenario 3, with an RP of 500 and an RQ of 800 produces the largest probable profit with a probability of stockout of less than 0.2.
A further MCS determined probable performance of this scenario over 24 months. The values chosen for the required parameters are shown in Table 9 and the MCS results in Table 10. This shows that with these parameters, the risk of loss over a 24 month period is 0% with a profit of £241,458.

Parameter	**Value**
Mean demand	500
Fixed order cost	£750
Unit cost	£25
Sales price	£45
Holding cost	£1
Salvage value	£25
Beginning inventory	800
Reorder point	500
Reorder quantity	800

Table 9: Parameters for 24 month inventory simulation.

Month	Beginning Inv.	Demand	Units Sold	End Inv.	Order Size	Order Cost (£)	Sales rev. (£)	Holding Cost (£)	Stockout?
1	800	486	486	314	800	£20,750	£21,870	£314	0
2	1114	548	548	566	0	£0	£24,660	£566	0
3	566	500	500	66	800	£20,750	£22,500	£66	0
4	866	478	478	388	800	£20,750	£21,510	£388	0
5	1188	500	500	688	0	£0	£22,500	£688	0
6	688	492	492	196	800	£20,750	£22,140	£196	0
7	996	526	526	470	800	£20,750	£23,670	£470	0
8	1270	532	532	738	0	£0	£23,940	£738	0
9	738	525	525	213	800	£20,750	£23,625	£213	0
10	1013	487	487	526	0	£0	£21,915	£526	0
11	526	518	518	8	800	£20,750	£23,310	£8	0
12	808	490	490	318	800	£20,750	£22,050	£318	0
13	1118	519	519	599	0	£0	£23,355	£599	0
14	599	508	508	91	800	£20,750	£22,860	£91	0
15	891	507	507	384	800	£20,750	£22,815	£384	0
16	1184	481	481	703	0	£0	£21,645	£703	0
17	703	517	517	186	800	£20,750	£23,265	£186	0
18	986	512	512	474	800	£20,750	£23,040	£474	0
19	1274	494	494	780	0	£0	£22,230	£780	0
20	780	478	478	302	800	£20,750	£21,510	£302	0
21	1102	520	520	582	0	£0	£23,400	£582	0
22	582	514	514	68	800	£20,750	£23,130	£68	0
23	868	495	495	373	800	£20,750	£22,275	£373	0
24	1173	494	494	679	0	£0	£22,230	£679	0
					Totals	£311,250	£545,445	£9,712	

Salvage value	£16,975

Any stockouts?	
0	

Total profit	£241,458

Table 10: Results of 24 month inventory simulation.

6. Mitigations

6.1. Cyber Mitigations

There is a 24% probability that one risk occurs in the 24-month period. Mitigations can be implemented to reduce this further:

1. Enforce stringent access controls and authentication (Ali et al, 2017).
2. Deploy Intrusion Detection and Prevention systems within the supply chain network (Deyannis, 2022).
3. Implement a robust patch management system (Boyson et al., 2022).
4. Exclusively obtain open-source software or data from reputable sources, seeking guidance from cybersecurity professionals ([1]Mitre, 2022).
5. Utilise secure communication protocols to transmit metadata between systems (Chhabra & Bajwa, 2015).

6.2. Disaster Mitigations

The risk of a disaster occurring is 100%. Therefore, it is important to take steps to reduce the impact on the business when a disaster occurs. Meteorological disasters produced the highest cost, suggesting that countries with lower meteorological disaster rates e.g., France, Spain & Italy, would be better to use as supplier areas. Given the inevitability of disasters and the need to tailor recommendations to specific infrastructure, which is unknown, it is recommended to establish an adequate number of geographically dispersed warehouses and suppliers. This distribution will allow the supply chain to remain resilient in the event of a disaster impacting one location.

6.3. Stock Recommendations

Managing inventory and hence supply chain resilience is crucial for business continuity and hence to mitigate potential losses (Christopher et al., 2004). To withstand and recover from potential risks, a business should build flexibility, redundancy, and agility into the supply chain (Sheffi, 2005). By using an MCS, Pampered Pets will be able to make informed decisions about the parameters of their proposed inventory management system to maximise efficiency.

Part II – Disaster Recovery

7. Disaster Recovery Plan (DRP)

A DRP is “A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.” (Stoufer et al., 2015). It is considered a subsection of a Business Continuity Plan which details critical functions of a business and how to maintain them following a disruptive event, within a specified timescale. Pampered Pets have specified a recovery time objective (RTO) and a restore point objective (RPO) of less than one minute. RPO defines the maximum acceptable data loss in case of a disaster, while RTO defines the maximum acceptable downtime.

The proposed DRP is valid with these assumptions (TCii Strategic and Management Consultants., 2012):

1. The business has identified key personnel to perform critical functions within the DRP.

2. Staff can be instantly notified and attend the designated backup point(s) to apply DRP procedures.

3. Staff members are sufficiently trained and familiar with the DRP and hence can perform their assigned roles effectively (ThinkSecure Network, 2021).

4. Alternate personnel are identified to cover in case primary staff members are unavailable.

These assumptions highlight the significance of having a dedicated DRP team (Spolia, 2019), and procedures to ensure their availability and effectiveness. By addressing these assumptions, an SME can be resilient in the face of potential disruptions.

Given the specifications of RTO<1 and RPO<1, a DRP will be implemented using an active-active system. It will feature a hot standby, with a blue system in operation and a green system on standby, as depicted in Figure 3 The green system will be immediately available for use.

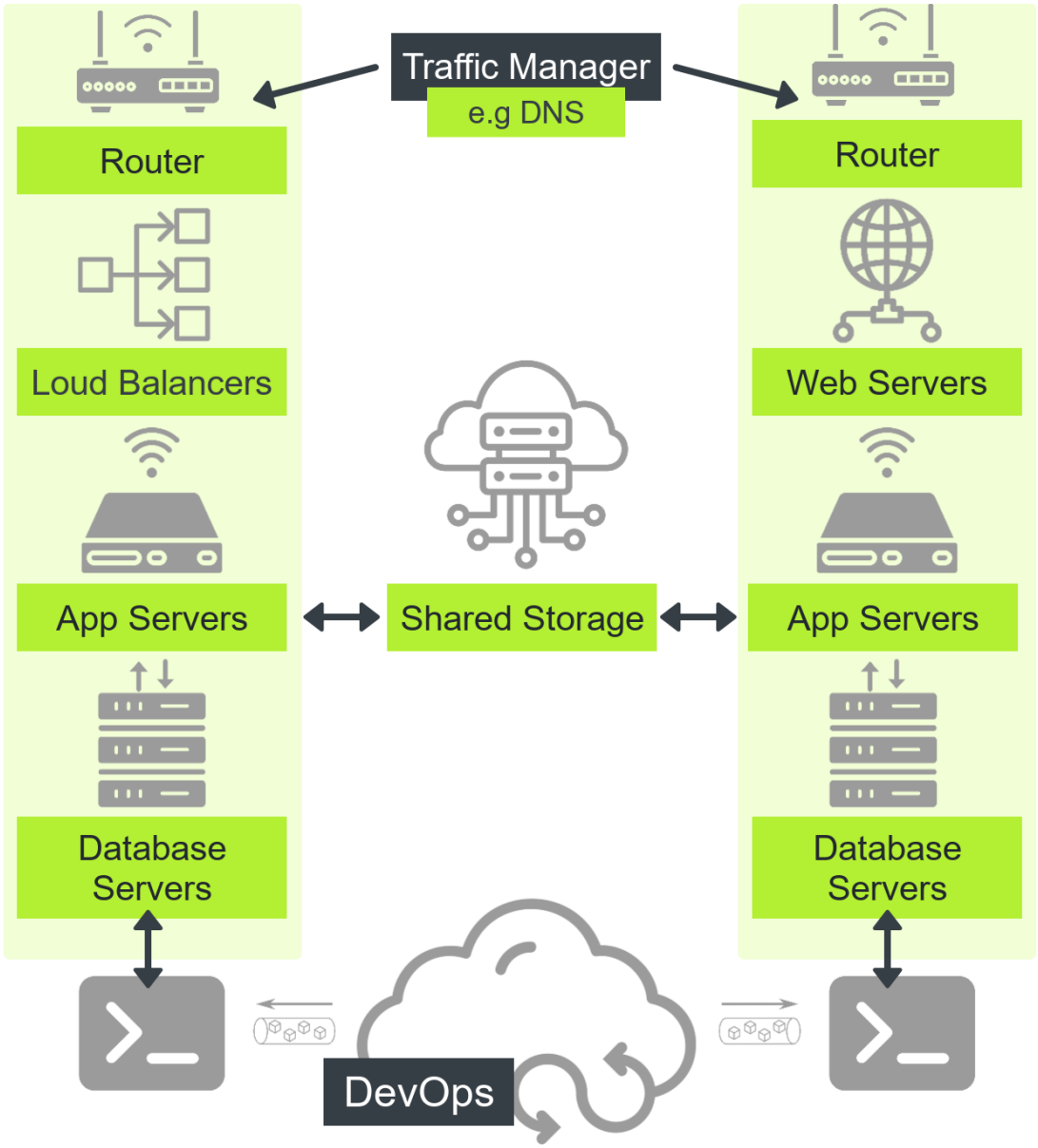

Figure 3: The proposed DR solution architecture. Modified after Millward, (2023).

8. Choosing a DRP

There are several types of Disaster Recovery solution available (Trovato et al., 2019)

- On-premises; backup and recovery systems set up locally for quick data restoration.
- Hybrid; combines on-premises and cloud-based solutions for scalability and cost savings.
- Multicloud - replicates data across multiple cloud platforms for greater redundancy and flexibility.
- Disaster Recovery as a Service (DRaaS); cloud-based disaster recovery that replicates data to a third-party cloud provider.

We recommend hosting the Pampered Pets e-commerce and DR solution on a cloud-based platform to ensure that e-commerce remains functional 24/7/365 and can be accessed from anywhere, even if the physical shop premises are unavailable.

DRaaS is a cloud-based solution providing a secondary site for data and application recovery where they can be recovered in the event of an outage or disaster (Andrade et al.,2017).

DRaaS provides the following advantages:

- High availability (Shulman, 2016).
- Resilience (Shulman, 2016).
- Simplified disaster recovery process.
- Optimised failover and fail-back (Shulman, 2016).
- It can be implemented without the requirement for specialised knowledge.
- No need to invest and maintain an offsite environment (Andrade et al.,2017)
- Flexible contracts according to the organisation needs (Andrade et al., 2017).

An example of DRaaS, Azure Industrial IoT, embraces Internet 4.0 principles to avoid vendor lock-in (Barnstedt, E., 2021). There are several reasons why Microsoft Azure is desirable (David, 2022), (Zimmergren et al., 2023):

- Integration with other Microsoft tools and services.
- Combine Artificial intelligence & Machine Learning.
- Strong security and compliance.
- Large community support.

9. Azure Site Recovery and VMWare Site Recovery Manager

Microsoft Azure will be used to create a DR solution for Pampered Pets, involving remote replication of the primary infrastructure and asynchronous backup of data. Azure Site Recovery (ASR) is a native DRaaS solution ideal for SMEs (Andrade et al., 2017). ASR offers easy deployment, cost-effectiveness, and reliability (Dutta et al.,2023). It will replicate Pampered Pets' virtual machines (VMs) to Azure, enabling automated failover and fail-back operations. A Virtual Network (VNet) in Azure will connect the on-premises environment to the Azure Cloud (Sudbring et al., 2023), see Figure 4.

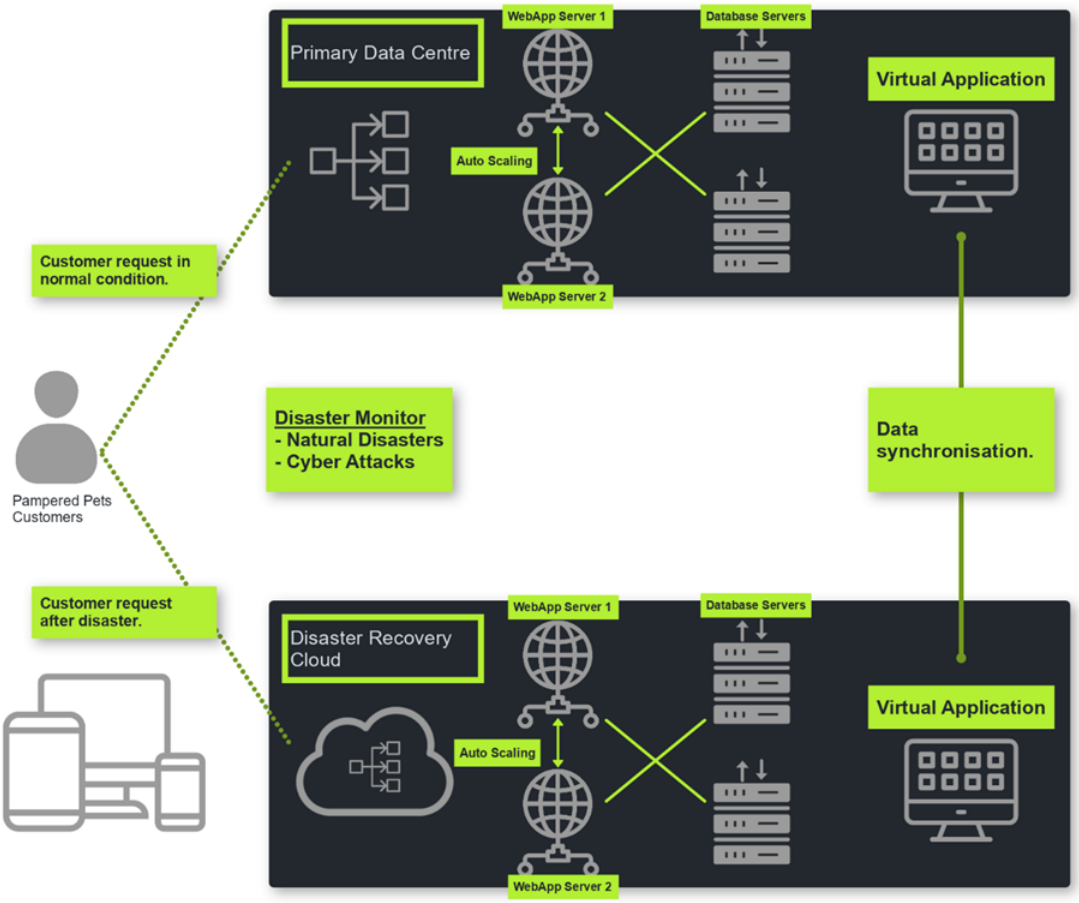

Figure 4 Proposed DRS for Pampered Pets. Modified after (Andrade et al.,2017).

For VM failover between sites, VMWare Site Recovery Manager (SRM) is recommended as it handles SRM installation and configuration, with the cloud provider responsible for infrastructure maintenance and supports recovery to Microsoft Azure (VMware Azure solution) (Cranney, 2021).

10. Azure and GDPR

General Data Protection Regulation (GDPR) can introduce complexities regarding the distribution of responsibilities between cloud providers and clients, which can vary depending on the service agreement in place.

If a data breach occurs due to a vulnerability in the cloud provider's infrastructure, both parties may have GDPR obligations (DPP-GDPR, N.D.). Regulatory authorities assess the situation based on the agreed-upon responsibilities and whether the provider implemented adequate security measures. Clear service agreements addressing GDPR compliance, including security measures and incident response protocols, are crucial (Tripwire, 2021).

Using the right tools to effectively manage GDPR compliance will help protect personal data and meet legal obligations and the recommended Azure platform provides a range of these (Pradeep, 2018); (Nair,2018). In addition to Azure tools, there are various online tools available to ensure GDPR compliance. For example, those provided by OneTrust, (OneTrust, 2021) and TrustArc, (TrustArc, 2021).

Azure undergoes regular third-party audits to validate its compliance with PCI DSS which required for e-commerce (Mazzoli et al., 2023) and essential for Pampered Pets. Azure also complies with other privacy standards such as HITRUST, EU-US Privacy shield, HIPAA/HITECH, EU Model Clauses, ISO/IEC 27018 (Pradeep, 2018); (Nair,2018).

11. Conclusion

The DRaaS model is an excellent disaster recovery technique, especially when implemented by a reputable provider. By reducing failure points, such as vendor lock-in, DRaaS models continue to advance industry 4.0 while maintaining flexibility. Assuring regulatory compliance, such as GDPR, allows organisations to quickly resume operations hence why it is our recommended DR solution for Pampered Pets to retain resilience against disasters.

References

Ali, W., et al (2017) ‘September. IoT based smart home: Security challenges, security requirements and solutions.’, *23rd International Conference on Automation and Computing,* pp.1-6.

Andrade, E., Nogueira, B., Matos, R., Callou, G. & Maciel, P. (2017) Availability modelling and analysis of a disaster-recovery-as-a-service solution. *Computing* 99(10): 929–954.

Barnstedt, E. (2021). 'How to Avoid Vendor Lock-In and Guide Your Industrial IoT Solutions', Microsoft Industry Blogs, 12 April 2021, Available at: https://www.microsoft.com/en-us/industry/blog/manufacturing/2021/04/12/how-to-avoid-vendor-lock-in-and-guide-your-industrial-iot-solutions/ [Accessed 15 May 2023].

Boyson, S., Corsi, T.M. & Paraskevas, J.P. (2022) ‘Defending digital supply chains: Evidence from a decade-long research program.’, *Technovation*, *118*, p.102380.

Butrimas, V. (2014) ‘National security and international policy challenges in a post Stuxnet world.’, *Lithuanian Annual Strategic Review*, *12*(1), pp.11-31.

Carabantes, D.S., Huidobro, C.B, & Vidal, D.C. (2016) ‘Optimation through Automation of Malware Update Process, Capable of Evading Anti-Malware Systems.’, *Research into Computer Science*, 127, pp.101-110.

Chhabra, G.S. & Bajwa, D.S. (2015) ‘Review of e-mail system, security protocols and email forensics.’, *International Journal of Computer Science & Communication Networks*, *5*(3), pp.201-211.

Christopher, M., & Peck, H. (2004) Building the resilient supply chain. *The International Journal of Logistics Management.* 15(2): 1-14.

Cranney, S. (2021) Disaster Recovery as a Service (DRaaS) in VMware – The Full Picture. Available from: https://www.altaro.com/vmware/disaster-recovery-as-a-service/ [Accessed 11 May 2023].

David, M. (2022) Benefits of Azure cloud services.Available from: https://www.simplilearn.com/azure-cloud-services-and-its-importance-article#benefits_of_azure_cloud_services [Accessed 15 May 2023].

Deyannis, D., Papadogiannaki, E., Chrysos, G., Georgopouloz, K., & Loannidis, S (2022) 'The Diversification and Enhancement of an IDS Scheme for the Cybersecurity Needs of Modern Supply Chains.', *Electronics*, *11*(13), p.1944.

DPP-GDPR. (N.D.) What You Should Know About Storing Data Under GDPR. Available from: https://www.dpp-gdpr.com/news/cloud-security-data-breach/ [Accessed 16 May 2023].

Dutta, A., & Pgaddala, V., & Jenks,A., & West, R., & Senthilna, V., & Juri, K., & Chishti, S., & Coulter, D., & Smatlak, D., & Wiselma, R., & Janaki, R., & Suaravarapu, V., &Jadi, E., & Caserio, C., & Kalso, P., & Fitz-Macken, T., & Boushev, G., & Sharma, P., & Lane, J (2023) Azure site recovery. Microsoft Azure. Available from: https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview [Accessed 6 May 2023].

Fahimnia, B., Tang, C.S, Davarzani, H., & Sarkis, J (2015) 'Quantitative models for managing supply chain risks: A review.', *European journal of operational research*, *247*(1), pp.1-15.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019) 'A retrospective impact analysis of the WannaCry cyberattack on the NHS.', *NPJ digital medicine*, *2*(1), p.98.

Ginting, G., Fadlina, M., Siahaan, A.P.U., & Rahim, R (2017) 'Technical approach of TOPSIS in decision making.' *International Journal of Recent Trends in Engineering & Research, 3*(8), pp.58-64.

Gray, D. & Ladig, J. (2015) 'The implementation of EMV chip card technology to improve cyber security accelerates in the US following target corporation's data breach.', *International Journal of Business Administration*, *6*(2), p.60.

Harrison, R.L. (2010) 'Introduction to Monte Carlo simulation.', *AIP conference proceedings*, 1204(1), pp. 17-21

Krasner, H. (2021) 'The cost of poor software quality in the US: A 2020 report.', *Consortium for Information and Software Quality.*

Mazzoli, R., Walker, C., Sriraman, MS., Buck, A. (2023) PCI DSS Compliance. Available from: https://learn.microsoft.com/en-us/compliance/regulatory/offering-pci-dss [Accessed: 15 May 2023].

Millward, D. (2023). *Business Continuity and Disaster Recovery* [Lecturecast]. SRM_PCOM7E March 2023 Security and Risk Management. University of Essex Online

[1]Mitre (2022) *CAPEC-693: StarJacking.* Available from: https://capec.mitre.org/data/definitions/693.html. [Accessed: 14 May 2023].

[2]Mitre (2022) *CAPEC Category:* Supply Chain*.* Available from: https://capec.mitre.org/data/definitions/437.html. [Accessed: 5 May 2023].

Nair, P. (2018) Protecting privacy in Microsoft Azure: GDPR, Azure Policy Updates. Available from: https://azure.microsoft.com/es-es/blog/protecting-privacy-in-microsoft-azure-gdpr-azure-policy-updates/ [Accessed 10 May 2023]

Olson, D.L. & Wu, D.D. (2010) *Enterprise risk management models* (No. 273102). Heidelberg: Springer.

OneTrust (2021) GDPR Compliance. OneTrust Blog. Available from: https://www.onetrust.com/blog/gdpr-compliance/ [Accessed 15 May 2023].

Pradeep, N. (2018) Protecting privacy in Microsoft Azure: GDPR, Azure Policy Updates. Available from: https://azure.microsoft.com/es-es/blog/protecting-privacy-in-microsoft-azure-gdpr-azure-policy-updates/ [Accessed 10 May 2023].

Resilinc. (2021) Supply Chain Disruptions up 67% in 2020 with Factory Fires Taking Top Spot for Second Year in a Row (2023). Available from: https://www.resilinc.com/press-release/supply-chain-disruptions-up-67-in-2020-with-factory-fires-taking-top-spot-for-second-year-in-a-row [Accessed: 18 May 2023].

Sheffi, Y. (2005). The resilient enterprise: Overcoming vulnerability for competitive advantage. MIT Press.

Shen, G. &Hwang, S.N. (2019) 'Spatial–Temporal snapshots of global natural disaster impacts Revealed from EM-DAT for 1900-2015.', *Geomatics, Natural Hazards and Risk*, *10*(1), pp.912-934.

Shulman, L.(2016) Disaster Recovery Journal. Disaster Recovery as a Service: Benefits and Challenges. Gartner. Available from: https://www.gartner.com/en/documents/3513817 [Accessed 12 May 2023].

Spolia, S. (2019) A Good Disaster Recovery Plan Has a Team in Place Before Disaster Strikes. Available from: https://www.supraits.com/disaster-recovery-plan-team/ [Accessed 16 May 2023].

Sudbring, A., & AL-Kazwini, H., & Bender, M., & Au, D. & Berry, D., & Dwivendi,K.,& Valivov, N., & Coulter, D., & Borsecnik, J., & Mabee, D., & Taylor, S., & Rabeler, C., & McGuire, C., & Mohamed, H., & Vasarapu, S., & Blythe, M., & Fitz-Maken,T., & Anavi, N., & Love, C., & Kuhtz, C., & Weinong, W., & Squllace, A., & Almeida, M., & Sampaio, T., & Nottingham, S., & Madureira, J., & Anamalai, N. (2023) Virtual networks overview. Available from: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview [Accessed 12 May 2023].

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. & Hahn, A. (2015) NIST Special Publication 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security. Available from: http://dx.doi.org/10.6028/NIST.SP.800-82r2 [Accessed 14th May 2023].

Tariq, M.I., Tayyaba, S., Ali Mian, N., Sarfraz, M.S., De-la-Hoz-Franco, E., S.A., Santarcangelo, V., & Rad, D.V. (2020) 'Combination of AHP and TOPSIS methods for the ranking of information security controls to overcome its obstructions under fuzzy environment.', *Journal of Intelligent & Fuzzy Systems*, *38*(5), pp.6075-6088.

TCii Strategic and Management Consultants. (2012) Writing a Disaster Recovery Plan. Available from: https://www.mondaq.com/uk/operational-performance-management/162946/writing-a-disaster-recovery-plan [Accessed 15 May 2023].

ThinkSecure Network. (2021) The Critical Need for Disaster Recovery, Business Continuity, and Prevention Strategy in Healthcare. Available from: https://www.thinksecurenet.com/blog/disaster-recovery-business-continuity-and-prevention-strategy-in-healthcare [Accessed 16 May 2023].

Tripwire. (2021) Impact of GDPR on Cloud Service Providers. Available from: https://www.tripwire.com/state-of-security/impact-of-gdpr-on-cloud-service-providers [Accessed 16 May 2023].

Trovato, F., & Sharp, A., & Siman,T. (2019) “Cloud, co-location, on-premises and hybrid disaster recovery solutions: Pros, cons, and a cost comparison.” *Journal of business continuity & emergency planning* vol. 13,2 (2019): 120-135.

TrustArc (2021) GDPR Compliance Solutions. TrustArc. Available from: https://trustarc.com/gdpr-compliance-solutions/ [Accessed 15 May 2023].

World Bank Group (2023) *Agriculture, forestry, and fishing, value added (% of GDP).* Available from: https://data.worldbank.org/indicator/nv.agr.totl.zs?most_recent_value_desc=false [Accessed: 5 May 2023].

Zimmergren, T., & Ekuan, M., & Bagby, R., & Moore, G., & Parker, D., & Buck, A., Coulter D. (2023) "How does Azure work". Microsoft Azure. Available from: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/what-is-azure [Accessed May 15, 2023].

Appendix 1

1.1: TOPSIS CALCULATIONS

The ‘Technique for Order of Preference by Similarity to Ideal Solution’ (TOPSIS) is a multi-criteria decision analysis method based on the concept that when given multiple criteria with possible solutions, the optimal solution is given by both the shortest geometric distance to the best solution for each criteria and the furthest distance to the worst solution for each criteria, within a defined evaluation matrix (Tariq et al, 2020).
To perform TOPSIS, we must assume that each criterion is monotonically increasing or decreasing, and that the criteria are independent of each other (Ginting et al, 2017). As such, it is appropriate to perform a TOPSIS calculation on ‘CAPEC Supply Chain Risk’ data, which identifies the cyber threats associated with a supply chain and their respective assessed likelihood of attack, typical severity and skill difficulty required to perform the attack (Mitre, 2022). This allows us to calculate which of these risks pose the highest overall threat to a supply chain and the overall risk of a successful attack.
A TOPSIS calculation can be performed using the following steps:

1. Create an “evaluation matrix” a_{ij} consisting of **M** alternatives and **N** criteria

$$\left(a_{ij}\right)_{M\times N}$$

2. Normalise the matrix by dividing each element by the square root of the sum of the squares of each element. Each element should now be between 0 and 1.

$$a_{ij} = \frac{a_{ij}}{\sqrt{\sum_{i=1}^{M} \left(a_{ij}\right)^2}}$$

3. Calculate the weighted normalised decision matrix, χ_{ij} , where each criterion is multiplied by its weight, and the weights from each criterion sum to 1.

4. Calculate the ideal worst values and ideal best values for each criterion. Together, the ideal worst values form the worst alternative, χ_i^w, and the ideal best values form the best alternative, χ_i^b.

5. For each element of the weighted normalised decision matrix, calculate the Euclidian distance to the best and worst alternative (d_i^b and d_i^w respectively).

$$d_i^b = \sqrt{\sum_{j=1}^{N} \left(\chi_{ij} - \chi_j^b\right)^2}$$

$$d_i^w = \sqrt{\sum_{j=1}^{N} \left(\chi_{ij} - \chi_j^w\right)^2}$$

6. For each alternative, calculate the performance score, s_i, which gives the similarity to the worst alternative using the distance to the best and worst alternative within the weighted normalised decision matrix.

$$s_i = \frac{d_i^w}{d_i^w + d_i^b}$$

7. Rank the alternatives in descending order based on their performance score.

To calculate the severity of a CAPEC Supply Chain attack, we implemented the following steps using the TOPSIS method:

1. For each attack, rank 'Likelihood of attack', 'Typical Severity', and 'Skill Level' between 1 and 5, for the corresponding given rank of 'Low' to 'Very high'. 'Skill Level' is given by the maximum skill difficulty required for an attack. Any missing data is given the lowest value, 'Low'.

	A	B	C	D	E	F	G	H
	Name	Likelihood Of Attack	Typical Severity	S	Skilled Level	Likelihood Value	Severity Value	Skilled Value
	Software Integrity Attack	Low	Low	:	Medium	1	1	2
	Malicious Software Download	Low	Very High	L	Low	1	4	1
	Malicious Software Update	Low	High	:	High	1	3	3
	Malicious Automated Software Update via Redirection	High	High	L	Low	3	3	1
	Signing Malicious Code	Low	Very High	L	Low	1	4	1
	Physically Hacking Hardware	Low	High	L	Low	1	3	1
	Bypassing ATA Password Security	Low	Low	L	Low	1	1	1

Figure A.1.1.1: CAPEC Supply Chain attack data with assigned Likelihood, Severity and Skill values

2. Following step (2) of the TOPSIS calculation, risks are squared and then normalised by dividing by the square root sum of the square

	A	I	J	K	L	M	N
	Name	Likelihood_value_squared	Severity_value_squared	Skilled_Value_Squared	Normalised_Likelikelihood	Normalised_Severity	Normalised_Skill
	Software Integrity Attack	=F2^2	=G2^2	=H2^2	=F2/SUM($I$2:$I$52)^0.5	=G2/SUM($J$2:$J$52)^0.5	=H2/SUM($K$2:$K$52)^0.5
	Malicious Software Download	=F3^2	=G3^2	=H3^2	=F3/SUM($I$2:$I$52)^0.5	=G3/SUM($J$2:$J$52)^0.5	=H3/SUM($K$2:$K$52)^0.5
	Malicious Software Update	=F4^2	=G4^2	=H4^2	=F4/SUM($I$2:$I$52)^0.5	=G4/SUM($J$2:$J$52)^0.5	=H4/SUM($K$2:$K$52)^0.5
	Malicious Automated Software Update via Redirection	=F5^2	=G5^2	=H5^2	=F5/SUM($I$2:$I$52)^0.5	=G5/SUM($J$2:$J$52)^0.5	=H5/SUM($K$2:$K$52)^0.5
	Signing Malicious Code	=F6^2	=G6^2	=H6^2	=F6/SUM($I$2:$I$52)^0.5	=G6/SUM($J$2:$J$52)^0.5	=H6/SUM($K$2:$K$52)^0.5
	Physically Hacking Hardware	=F7^2	=G7^2	=H7^2	=F7/SUM($I$2:$I$52)^0.5	=G7/SUM($J$2:$J$52)^0.5	=H7/SUM($K$2:$K$52)^0.5

Figure A.1.1.2: Excel formulas used for calculating normalised likelihood, severity and skill values for CAPEC Supply Chain attack data.

3. As TOPSIS assesses the risk of a successful attack, it is assumed that the likelihood of attack, severity of attack, and skills required to carry out an attack all contribute appropriately equally to whether an attack is successful and the risk to the organisation posed by it. As such, each of these variables were equally weighted.
4. The Ideal Best and Worst values for each of the three variables were calculated using MAX() and MIN() Excel functions.

R	S
Ideal_Best_Likelihood	**Ideal_Worst_Likelihood**
0.295598783	0.098532928
Ideal_Best_Severity	**Ideal_Worst_Severity**
0.186907725	0.046726931
Ideal_Best_Skill	**Ideal_Worst_Skill**
0.058123819	0.174371458

Figure A.1.1.3: Ideal best and worst values found for Likelihood, Severity and Skill as part of the TOPSIS calculation.

The distance to the ideal best and ideal worst was calculated and then the performance score was calculated for each attack. The attacks were then sorted in descending order based on the performance score.

A	O	P	Q
Name	**Distance to Ideal Best**	**Distance to Ideal Worst**	**Performance Score**
Software Integrity Attack	=(($R$2-L2)^2+($R$4-M2)^2+($R$6-N2)^2)^0.5	=(($S$2-L2)^2+($S$4-M2)^2+($S$6-N2)^2)^0.5	=P2/(O2+P2)
Malicious Software Download	=(($R$2-L3)^2+($R$4-M3)^2+($R$6-N3)^2)^0.5	=(($S$2-L3)^2+($S$4-M3)^2+($S$6-N3)^2)^0.5	=P3/(O3+P3)
Malicious Software Update	=(($R$2-L4)^2+($R$4-M4)^2+($R$6-N4)^2)^0.5	=(($S$2-L4)^2+($S$4-M4)^2+($S$6-N4)^2)^0.5	=P4/(O4+P4)
Malicious Automated Software Update via Redirection	=(($R$2-L5)^2+($R$4-M5)^2+($R$6-N5)^2)^0.5	=(($S$2-L5)^2+($S$4-M5)^2+($S$6-N5)^2)^0.5	=P5/(O5+P5)
Signing Malicious Code	=(($R$2-L6)^2+($R$4-M6)^2+($R$6-N6)^2)^0.5	=(($S$2-L6)^2+($S$4-M6)^2+($S$6-N6)^2)^0.5	=P6/(O6+P6)

Figure A.1.1.4: Excel formulas used for calculating distance to ideal best and ideal worst for each attack as part of the TOPSIS calculation and the formula used for calculating the performance score for each attack.

5. The percentage chance of a successful attack for each attack was approximated by assuming a linear relationship with the performance scores and assuming that it is highly likely that at least one attack would be successful. As such, each probability was found by dividing each performance score by the sum of performance scores. This method reflects that the likelihood, severity, and skill level required to perform the attack will all factor in the likelihood of the attack being successful.
6. For simplicity, the nine attacks with the top performance score were used in the Monte Carlo Simulation to calculate the overall threat of a cyber-attack. Attacks with high likelihood and severity, and low skill level required were found to pose the greatest cyber threat to supply chains.

A	B	C	D	E	F
Name	**Likelihood Of Attack**	**Typical Severity**	**Skill Level**	**Performance Score**	**Probability of successful attack**
Malicious Automated Software Update via Redirection	High	High	Low	0.84	4%
Malicious Automated Software Update via Spoofing	High	High	Low	0.84	4%
Malicious Logic Inserted Into Product by Authorized Developer	Medium	High	Low	0.62	3%
Development Alteration	Medium	High	Low	0.62	3%
Malicious Logic Insertion into Product Software via Configuration Management Manipulation	Medium	High	Low	0.62	3%
Malicious Logic Insertion into Product via Inclusion of Third-Party Component	Medium	High	Low	0.62	3%
Design Alteration	Medium	High	Low	0.62	3%
StarJacking	Medium	High	Low	0.62	3%
Metadata Spoofing	Medium	High	Medium	0.54	3%

Figure A.1.1.5: Final table from the TOPSIS calculation showing a sorted list of the top nine cyber-attacks by performance score, and probability of a successful attack associated with these risks.

Appendix 1.2: FINANCIAL IMPACT RESEARCH

Formulating an accurate assessment of the tangible economic impact of a specific cyber-attack on a company is a costly and intricate undertaking (Carabantes et al., 2016). Therefore, research was conducted to find an average cost to companies for these costs. Where costs were not publicly available, a cost of $1,000,000.00 was assigned as a use value. The final values are as follows:

- Malicious Automated Software Update □ $21,041,666.66 (Krasner, 2021)
- Malicious Logic Inserted □ $52,950,000.00 (Ghafur et al, 2019) (Gray & Ladig, 2015)
- Alterations (Design and Development) □ $10,000,00.00 (Butrimas, 2014)
- Starjacking □ $1,000,000.00
- Metadata Spoofing □ $1,000,000.00

Appendix 2

2.1: SUPPLY CHAIN ASSUMPTIONS

To access the supply chain risks, simplifications were employed to focus on the most pertinent data. The following assumptions were made:

- The assessment of supply chain data was primarily based on European data, considering the presence of high-profile customers from that region.
- Cross-border transportation is facilitated by the freedom of movement, with the impact of Brexit not considered due to the lack of recent historical data.
- The analysis assumes no further pandemic-related disruptions beyond the available historical data, as it is unlikely for another event to affect the world in the same manner.
- It is assumed that no significant regulatory changes will impact the supply chains of different countries. Any potential alterations that could necessitate a complete overhaul of the business model are considered beyond the scope of this report.

2.2: DISASTER DATA PROCESS

Data was collected from the EM-DAT database, and average values were calculated. This is shown in Figure A.2.2.1 and A.2.2.2

Disaster Occurences						
Disaster	France	Germany	Italy	Netherlands	Spain	China
Geophysical	2	3	35	1	2	168
Hydrological	66	23	57	4	35	371
Climatological	17	1	14	0	22	46
Meteorological	96	73	39	34	36	325
Biological	2	2	2	1	3	8
Technological	70	49	90	18	67	965

Figure A.2.2.1 : Disaster occurrences

Total estimated damages						
Country	Geophysical	Hydrological	Climatological	Meteorological	Biological	Technological
France	$0	$18,094,326,000	$3,810,425,000	$62,258,842,000	$0	$121,761,000
Germany	$795,819,000	$86,154,451,000	$0	$57,165,834,000	$0	$1,153,387,000
Italy	$132,383,483,000	$44,895,613,000	$9,492,200,000	$19,201,964,000	$0	$8,451,000
Netherlands	$0	$1,116,464,000	$0	$9,380,242,000	$0	$855,200,000
Spain	$337,518,000	$27,009,364,000	$29,836,475,000	$11,585,623,000	$0	$16,608,655,000
China	$177,272,693,000	$471,227,009,000	$919,098,531,000	$202,080,732,000	$0	$464,269,000

Figure A.2.2.2: Disaster Costs.

Then this was collated for each risk, shown in Figures A.2.2.3 - A.2.2.5

Geophysical				
Country	Rate per year	Rate per 24 months	Aveagre Cost	24 Month Cost Estimate
France	0.04	0.08	$0	$0
Germany	0.06	0.12	$265,273,000	$31,832,760
Italy	0.7	1.4	$3,782,385,228.57	$5,295,339,320
Netherlands	0.02	0.04	$0	$0
Spain	0.04	0.08	$168,759,000	$13,500,720
China	3.36	6.72	$1,055,194,601.19	$7,090,907,720

Hydrological				
Country	Rate per year	Rate per 24 months	Aveagre Cost	24 Month Cost Estimate
France	1.32	2.64	$274,156,454.55	$723,773,040.00
Germany	0.46	0.92	$3,745,845,695.65	$3,446,178,040.00
Italy	1.14	2.28	$787,642,333.33	$1,795,824,520.00
Netherlands	0.08	0.16	$279,116,000	$44,658,560.00
Spain	0.7	1.4	$771,696,114.29	$1,080,374,560.00
China	7.42	14.84	$1,270,153,663.07	$18,849,080,360.00

Figure: A.2.2.3 : Geographical and Hydrological data

Climatological				
Country	Rate per year	Rate per 24 months	Aveagre Cost	24 Month Cost Estimate
France	0.34	0.68	$224,142,647.06	$152,417,000.00
Germany	0.02	0.04	$0	$0
Italy	0.28	0.56	$678,014,285.71	$379,688,000.00
Netherlands	0	0	0	0
Spain	0.44	0.88	$1,356,203,409.09	$1,193,459,000.00
China	0.92	1.84	$19,980,402,847.83	$36,763,941,240.00

Meteorological				
Country	Rate per year	Rate per 24 months	Aveagre Cost	24 Month Cost Estimate
France	1.92	3.84	$648,529,604.17	$2,490,353,680.00
Germany	1.46	2.92	$783,093,616.44	$2,286,633,360.00
Italy	0.78	1.56	$492,358,051.28	$768,078,560.00
Netherlands	0.68	1.36	$275,889,470.59	$375,209,680.00
Spain	0.72	1.44	$321,822,861.11	$463,424,920.00
China	6.5	13	$621,786,867.69	$8,083,229,280.00

Figure: A.2.2.4 : Climatological and Meteorological data

Biological

Country	Rate per year	Rate per 24 months	Aveagre Cost	24 Month Cost Estimate
France	0.04	0.08	0	0
Germany	0.04	0.08	0	0
Italy	0.04	0.08	0	0
Netherlands	0.02	0.04	0	0
Spain	0.06	0.12	0	0
China	0.16	0.32	0	0

Technological

Country	Rate per year	Rate per 24 months	Aveagre Cost	24 Month Cost Estimate
France	1.4	2.8	$1,739,442.86	$4,870,440.00
Germany	0.98	1.96	$23,538,510.20	$46,135,480.00
Italy	1.8	3.6	$93,900	$338,040.00
Netherlands	0.36	0.72	$47,511,111.11	$34,208,000.00
Spain	1.34	2.68	$247,890,373.13	$664,346,200.00
China	19.3	38.6	$481,107.77	$18,570,760.00

Figure: A.2.2.5 : Biological and Technological data

Based on the available data, the decision was made to exclude biological data due to limited information regarding the associated cost of such disasters. Additionally, the decision was taken to disregard the data collected from China, as it presented notable disparities when compared to the European data. Given that the security-focused clients hail from Europe, ensuring accuracy aligned with that region is of most importance.
Final calculations were undertaken to produce parameters for a Monte Carlo simulation. An assumption was made that a single company would not have damages of over 1% of the total disaster costs to a single country. These are shown in Figure A.2.2.6.

Disaster	Average Rate per 24 Months	Percentage chance of at least one disaster	Average Cost per 24 Months	Estimated cost per 24 months
Geophysical	0.34	0.29107107195049	$1,068,134,560	$10,681,345.60
Hydrological	1.48	0.77236231161619	$1,418,161,744.00	$14,181,617.44
Climatological	0.43	0.35079062331485	$106,421,000.00	$1,064,210.00
Meteorological	2.22	0.89182445989481	$1,276,740,040.00	$12,767,400.40
Technological	2.35	0.90482138549765	$149,979,632.00	$1,499,796.32

Figure A.2.2.6: Calculated Parameters.

Appendix 3

Stock and Costing Data

Presenting the complete data set used to produce the summaries shown of agricultural production and price data would be inappropriate in printed format due its size. Therefore, the full crop production data set is provided in separate file called **Agri_production_data.xlsx**

Appendix 4

Appendix 4.1: MCS RISK WORKINGS

A Monte-Carlo simulation was used to calculate the percentage chance of at least one disruption caused by either risks posed by cyber threats or natural disasters, and what the expected cost of that disruption would be along with a 90% confidence interval.
A Monte-Carlo simulation uses repeated random sampling to model complex systems which often do not have clear analytical solutions (Harrison, 2010). The simulation assumes that the random variables being sampled are independent of each other.
To perform the simulation, the top cyber risks associated with supply chain disruption were calculated using the TOPSIS method, along with the likelihood of a successful attack and what the financial impact would be in a reasonable worst-case scenario. It was assumed that a reasonable worst-case scenario for an attack lies at the 90th percentile of the distribution.
The probability of a natural disaster for each type (Geophysical, Hydrological, Climatological, Meteorological, Technological) was calculated using the average rate of these disasters. The financial impact was estimated by finding the average impact of these disasters and assuming the average impact lies at the 50th percentile of the distribution.
Using the reasonable worst-case impact for a cyber-attack and average impact for a natural disaster, log-normal distributions were created to model the potential financial impact of a cyber-attack or natural disaster. These distributions had varying mean values and, for simplicity, had set standard deviations of 1, for the respective normal distribution.
The expected cost of each disruption risk was randomly sampled 1000 times. The expected cost of a disruption risk was found by multiplying the probability that there would be disruption by the potential cost of that disruption. The RAND() function was used to sample whether there was disruption in each case (1 if there was, but otherwise 0). The cumulative inverse lognormal LOGNORM.INV() function was used to sample the impact of that disruption by randomly sampling up to the 95th percentile (assumed absolute worst-case scenario as the cumulative inverse lognormal function tends to infinity as the cumulative probability tends to one).

R	S	T
Attack 1 successful?	**Cost of Succesful Attack 1**	**Expected Cost of Attack 1**
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R2*S2
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R3*S3
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R4*S4
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R5*S5
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R6*S6
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R7*S7
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R8*S8
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R9*S9
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R10*S10
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R11*S11
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R12*S12
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R13*S13
=IF(RAND()<0.042, 1, 0)	=LOGNORM.INV(RANDBETWEEN(0, 0.95*1000)/1000, 1.77,1)	=R14*S14

Figure x: Snapshot of the Excel formulas used to simulate the expected cost of a successful cyber attack or natural disaster.

The total expected cost for each sample was found by summing the expected cost of each risk. This was also separately summed for just the cyber risks and natural disaster risks. The percentage chance of disruption was calculated by finding the

proportion of samples which had at least one disruption. The expected impact was calculated by taking the average financial impact of the samples which had at least one disruption, and the 90% confidence interval was calculated by sorting the data with at least one disruption by the financial impact of the disruption in ascending order, and manually finding where 90% of the data fell.

4.2: MCS STOCK WORKINGS

An MCS was performed using the YASAI[1] Excel add in, to determine the probable mean profit and chance of stockout of various combinations of RP and RQ values. 1000 simulations of each scenario were performed. The figures below show a snapshot of the simulation output.

YASAI Simulation Output

Workbook	pampered_pets_inventory_simulation.xls	**YASAI Version:**	3
Sheet	Formulas	**Use Same Seed?**	Yes
Start Date	01/05/2023	**Random Number Seed:**	1
Start Time	11:47:44 AM		
Run Time (h:mm:ss)	00:00:08		
Scenarios:	7		
Sample Size:	1000		

	Parameter	
Scenario	Reorder point	Reorder quantity
1	400	500
2	500	700
3	500	800
4	500	1000
5	600	700
6	600	1000
7	700	2000

Output Name	Scenario	Observations	Mean	Standard Deviation	Minimum	5th Percentile	10th Percentile	15th Percentile	20th Percentile	25th Percentile	30th Percentile
Any stockouts?	1	1000	0.309	0.462	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Any stockouts?	2	1000	0.269	0.444	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Any stockouts?	3	1000	0.196	0.397	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Any stockouts?	4	1000	0.027	0.162	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Any stockouts?	5	1000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Any stockouts?	6	1000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Any stockouts?	7	1000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Total profit	1	1000	235575.266	2761.562	228769.000	231723.150	232507.800	232975.550	233343.600	233691.250	233917.700
Total profit	2	1000	238600.809	2176.708	230628.000	234984.300	235971.300	236523.850	236910.400	237254.750	237561.800
Total profit	3	1000	239120.091	2239.508	231228.000	235425.450	236397.100	237102.200	237488.400	237775.500	238108.100
Total profit	4	1000	237931.141	3366.151	230535.000	232662.650	233591.500	234257.800	234851.800	235368.000	236099.300
Total profit	5	1000	236271.453	2163.984	228528.000	232573.250	233720.500	234212.000	234588.200	234866.000	235160.200
Total profit	6	1000	237659.803	3426.239	226840.000	231685.350	233061.800	234119.950	234754.600	235344.500	236080.400
Total profit	7	1000	229211.553	2726.438	217978.000	224185.350	225541.000	226446.850	227105.400	227595.250	228133.000

Figure A.4.2.1: Example of the MCS output for the various RP and RO Scenarios.

[1] http://www.yasai.rutgers.edu/

The best scenario was then used to run an MCS of an inventory system for a 24 month period. The screenshot below shows a snapshot of the formulas used to produce this. The full simulation data is provided in the file:
pampered_pets_inventory_simulation.xlsx

Simulation of 24-month period					
Month	Beginning Inv	Demand	Units Sold	End Inv	Order Size
1	=C11	=@genPoisson(C$3)	=MIN(C19,B19)	=B19-D19	=IF(E19<=$C$13,$C$14,0)
2	=E19+F19	=@genPoisson(C$3)	=MIN(C20,B20)	=B20-D20	=IF(E20<=$C$13,$C$14,0)
3	=E20+F20	=@genPoisson(C$3)	=MIN(C21,B21)	=B21-D21	=IF(E21<=$C$13,$C$14,0)
4	=E21+F21	=@genPoisson(C$3)	=MIN(C22,B22)	=B22-D22	=IF(E22<=$C$13,$C$14,0)
5	=E22+F22	=@genPoisson(C$3)	=MIN(C23,B23)	=B23-D23	=IF(E23<=$C$13,$C$14,0)
6	=E23+F23	=@genPoisson(C$3)	=MIN(C24,B24)	=B24-D24	=IF(E24<=$C$13,$C$14,0)
7	=E24+F24	=@genPoisson(C$3)	=MIN(C25,B25)	=B25-D25	=IF(E25<=$C$13,$C$14,0)
8	=E25+F25	=@genPoisson(C$3)	=MIN(C26,B26)	=B26-D26	=IF(E26<=$C$13,$C$14,0)
9	=E26+F26	=@genPoisson(C$3)	=MIN(C27,B27)	=B27-D27	=IF(E27<=$C$13,$C$14,0)
10	=E27+F27	=@genPoisson(C$3)	=MIN(C28,B28)	=B28-D28	=IF(E28<=$C$13,$C$14,0)
11	=E28+F28	=@genPoisson(C$3)	=MIN(C29,B29)	=B29-D29	=IF(E29<=$C$13,$C$14,0)
12	=E29+F29	=@genPoisson(C$3)	=MIN(C30,B30)	=B30-D30	=IF(E30<=$C$13,$C$14,0)
13	=E30+F30	=@genPoisson(C$3)	=MIN(C31,B31)	=B31-D31	=IF(E31<=$C$13,$C$14,0)
14	=E31+F31	=@genPoisson(C$3)	=MIN(C32,B32)	=B32-D32	=IF(E32<=$C$13,$C$14,0)
15	=E32+F32	=@genPoisson(C$3)	=MIN(C33,B33)	=B33-D33	=IF(E33<=$C$13,$C$14,0)
16	=E33+F33	=@genPoisson(C$3)	=MIN(C34,B34)	=B34-D34	=IF(E34<=$C$13,$C$14,0)
17	=E34+F34	=@genPoisson(C$3)	=MIN(C35,B35)	=B35-D35	=IF(E35<=$C$13,$C$14,0)
18	=E35+F35	=@genPoisson(C$3)	=MIN(C36,B36)	=B36-D36	=IF(E36<=$C$13,$C$14,0)
19	=E36+F36	=@genPoisson(C$3)	=MIN(C37,B37)	=B37-D37	=IF(E37<=$C$13,$C$14,0)
20	=E37+F37	=@genPoisson(C$3)	=MIN(C38,B38)	=B38-D38	=IF(E38<=$C$13,$C$14,0)
21	=E38+F38	=@genPoisson(C$3)	=MIN(C39,B39)	=B39-D39	=IF(E39<=$C$13,$C$14,0)
22	=E39+F39	=@genPoisson(C$3)	=MIN(C40,B40)	=B40-D40	=IF(E40<=$C$13,$C$14,0)
23	=E40+F40	=@genPoisson(C$3)	=MIN(C41,B41)	=B41-D41	=IF(E41<=$C$13,$C$14,0)
24	=E41+F41	=@genPoisson(C$3)	=MIN(C42,B42)	=B42-D42	=IF(E42<=$C$13,$C$14,0)
					Totals
Salvage value	=$C$9*(E42+F42)				
			Any stockouts?		
Total profit	=@simOutput(H43+B44-G43-I43,A46		=@simOutput(IF(SUM(J19:J42)>0,1,0),D45		

Figure A.4.2.2: Screenshot showing part of the formulas used to produce the 24 month inventory simulation.