Julius Cloos
Security and Risk Management
Tutor: Dr. Siddiqui

Executive Summary

Following the Risk Identification Report, Pampered Pets requested a detailed analysis of its risk exposure, as well as recommendations for the integration of its new manufacturing and distribution center into the existing disaster recovery (DR) strategy.

This report will first describe the most relevant risks to the business, followed by a quantitative analysis of the risks. After then outlining the benefits and drawbacks of cloud-based DR strategies, this report will show a possible way to integrate the new center into the existing DR strategy. Furthermore, the benefits of failover clusters are discussed to provide Pampered Pets with a way to shorten its Return Point Objective (RPO) and Return To Operations (RTO) times (under specific circumstances).

This report will also analyze GDPR-related and PCI-DSS related issues which must be considered as part of the DR strategy, specifically the requirement to keep user data on servers in certain countries and to secure user data against unintentional losses.

Risks to Business Operations

Supply chain risks have increased greatly in the last years due to the increased interdependency of companies worldwide. Globalization is responsible for a major increase in the complexity of supply chains as warehouses, production facilities and distribution centers are scattered across the entire planet (Gimenez, 2016). The tendency is that the complexity will increase more, as rigid and linear supply chains get transformed into more complex supply networks (Gimenez, 2016). Managing the risks associated with supply chain disruptions will therefore become even more prudent.

To assess the risks for Pampered Pets, this report will use a Monte-Carlo Simulation. A Monte-Carlo Simulation is a mathematical tool which helps to predict the outcomes of uncertain events by supplying a model with random inputs (IBM, N.D.). This report used a Monte-Carlo Simulation to assess how many different risks are likely to affect Pampered pets. The methodology was as follows:

1. Gather data on the likelihood of different risks occurring. This report uses data from Rudden (2024).
2. To gain a more representative view on the data, the average probability of a risk occurring from 2022 to May 2024 was used. French et. al. (2011) outlines this is useful for reducing instabilities (i.e. heavy variances) between different data points.
3. 10 000 trials were executed, with each trial testing if a risk occurred by using its percentage probability from step 2.
4. The number of cases where the risks occurred was calculated.

The result, as seen in Figure 1, of this Monte-Carlo Simulation indicates that Pampered Pets will almost certainly (95%) be affected by at least 1 of the following risks:

- Cyber attacks
- Business interruptions
- Natural catastrophes
- Changes in legislation and regulation
- Macroeconomic developments

- Climate change
- Energy crises
- Fires/Explosions
- Market developments
- Labor shortages
- Political risks
- Pandemics
- Critical infrastructure blackouts
- New technologies
- Loss of reputation
- Theft
- Product recall
- Insolvency
- Environmental risks

Fig. 1: Chart showing the probability of different numbers of risks affecting the company. Created using Microsoft Excel.

Figure 1 clearly shows that adequate risk management is a necessity. To prove the statistical significance of the results above, another simulation was executed:

1. Run a simulation as described before to calculate the percentage for at least 1 risk happening.
2. Record that value and re-run the simulation for 10 000 iterations.

The histogram in Figure 2 shows the statistical significance of the data, given the small standard deviation of 0.2% and the probability of 1 or more risks occurring was never lower than 94.76%.

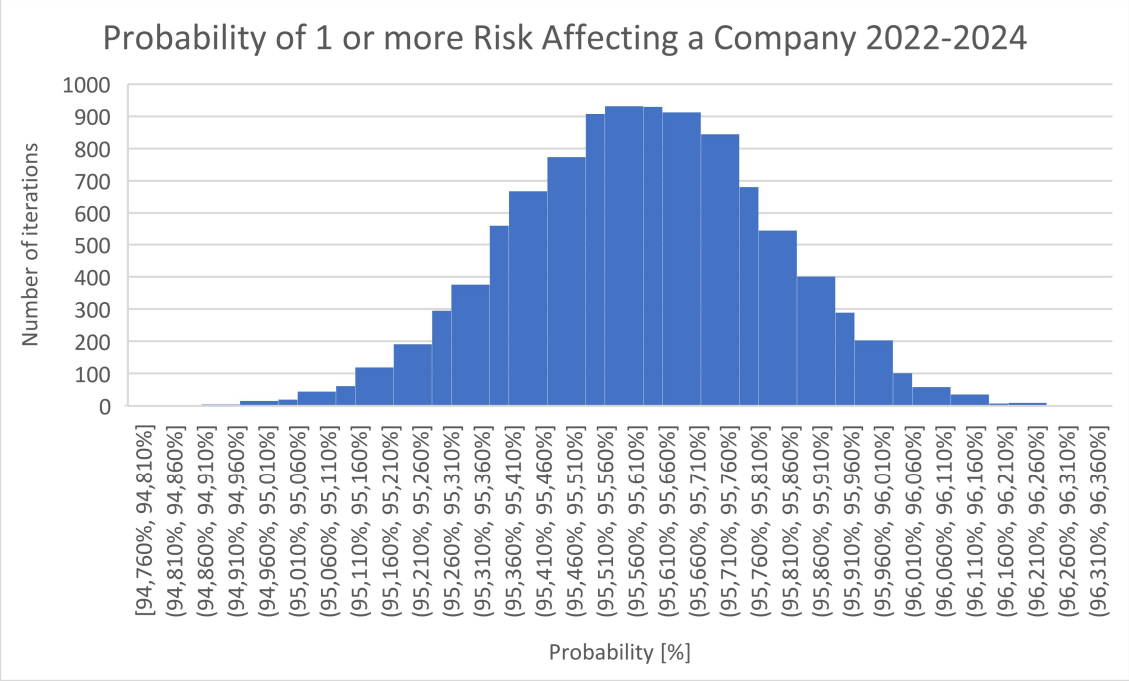

Fig. 2: Histogram of the distribution of probabilities for 1 or more risks affecting the company. Created using Microsoft Excel.

Unfortunately, this simulation has multiple weaknesses, which need to be considered when interpreting the results:

- Different risks have different probabilities of happening at different locations in the world. For example, geographical and developmental factors play a large role in how prone a country is to risks from natural disasters (Charvériat, 2000).
- Some risks are likely to increase. For example, climate change is likely going to become more and more of a concern (Bititci et. al., 2020). Given new facilities are long-term investments, especially for a SME like Pampered Pets, the increase of risks over time should be considered.
- Businesses who depend on supply chains from (or going through) unstable areas in the world will likely face increased risks to their supply chain. This can be due to increased risks from terrorism, political instability or shifting economic policies (Albin et. al., 2006).

Necessity of DR strategies

A functional DR strategy is not only a benefit to the organization, but also necessary due to regulatory standards. For example, Art. 32 of GDPR requires businesses to ensure that personal data can be recovered in case of disasters (Bültmann, 2022). GDPR violations can be very expensive, as they can be up to 4% or 20 million EUR in severe cases (Wolford, 2024). This can be crippling to SMEs such as Pampered Pets. This alone provides ample justification for the implementation of a functional DR strategy, even ignoring business risks such as the loss of stored foodstuff.

Julius Cloos
Security and Risk Management
Tutor: Dr. Siddiqui

Benefits and Drawbacks of Cloud-Based DR strategies

The current DR strategy of Pampered Pets allows 24/7 availability for the online shop, as well as a 1-minute changeover window in case of a disaster and a maximum data loss of 1 minute. Also, the DR-strategy is cloud based. Cloud-based systems have multiple benefits compared to on-premises systems. Especially for an SME, the costs of purchasing and maintaining redundant physical servers across multiple locations can be problematic. Given the short changeover window, it is assumed Pampered Pets is already using a cloud-based Disaster-Recovery-as-a-Service (DRaaS) provider, as even "hot site" (meaning the backup system needs to be ready to process production-load requests immediately once the main system has failed) systems require changeover-windows longer than 1 minute (Abualkishik, 2020).

Lower costs for servers and IT-staff are not the only advantages of cloud-based DR-strategies, however. Other advantages include the fact that a business can avoid the workload maintaining redundant systems (Abualkishik, 2020).

Unfortunately, there are also disadvantages of using cloud computing. For example, business become dependent on the cloud provider (Abualkishik, 2020). Changing providers can be difficult, especially once the business has integrated many of the cloud provider's unique tools etc. This is known as vendor lock-in. Vendor lock-in can become a serious problem when issues arise such as a decline in the quality of the services the provider provides and the cloud provider changing the services to a point where the service becomes useless to the business (Cloudflare, 2024).

The more severe disadvantage, however, is that businesses may have no control over the location of the servers storing or processing the data (Abualkishik, 2020). For example, GDPR requires that sensitive data about European users to be stored in the European Union (SealMetrics, 2024). If the cloud provider runs the database containing sensitive data about European users outside the EU, there may be large penalties for the business. In 2023, Meta was sentenced to pay a 1.2 billion EUR penalty after they had illegally transferred data about European citizens to the United States (InCountry, 2024).

Integrating the New Facility

According to Pampered Pets management, the DR strategy needs to ensure a RPO of 1 minute and a RTO of 1 hour. This report assumes the following systems will be present in the new warehouse/distribution/manufacturing center:

- Warehouse Management System to control daily warehouse operations (Thahiba et. al., 2022)
- Systems to control distribution of goods
- Systems required to manufacture goods

For simplicity, the systems for controlling distribution and manufacturing will each be considered as 1 server, given Pampered Pets has not provided detailed information on their requirements regarding these systems. However, the proposed strategy can easily be extended to include more systems (one of the major benefits of cloud-based DR strategies).

Julius Cloos
Security and Risk Management
Tutor: Dr. Siddiqui
Given Pampered Pets management has not provided any details on the systems it will use in its new center, this report will assume these are the systems needed to be included in the DR-strategy. If necessary, other systems can be included later at minimal cost. This is one of the major advantages of cloud-based DR-strategies (Abualkishik et. al., 2020).

Furthermore, Pampered Pets management decided the new site needs to include environmental and physical security monitoring. These systems also need to be included in the DR-strategy, because especially video feeds from surveillance cameras can be very useful in disaster situations, as they can increase situational awareness and improve the decision-making process by allowing emergency teams a better overview of the disaster-affected area (Grecos et. al., 2012). Therefore, efforts should be made to allow access to the video cameras during a disaster. Also, the recordings should be saved off-site given an intruder could steal or destroy the video surveillance footage otherwise (Ahmad et. al., 2020).

While this report isn't going to delve into the technical details, it is recommended that Pampered Pets uses WPA3-Enterprise access points. WPA3-Enterprise improves on several aspects of WPA2-Enterprise, for example by increasing the encryption key lengths (Akhtar et. al., 2022). This contributes to reducing the risks posed by wireless-based attacks. Further technical details on infrastructure requirements, such as the presence of a web-application firewall for potential cloud-based web shops due to PCI-DSS, as described by Davies (2024), are omitted from this report, as this would be out-of-scope for this executive summary.

The requirement of having a 1-minute RPO means the business will likely continue to use a DRaaS-based DR strategy. Theoretically, the business could use failover-cluster configurations for the critical systems, maintaining backup systems in the cloud incase the physical servers are lost to a disaster. A failover-cluster consists of multiple servers, ensuring that another server ("node") can take over upon failure of other nodes and a load balancer which controls which node receives requests. Studies such as the one completed by Dewantara et. al. (2018) suggest that data losses can be kept in the millisecond-range. Of course, this would be advantageous for the business, however, it would at least double the number of servers (and add additional servers as load balancers). Also, there would still need to be cloud-based backup systems if the entire site suffers a major disaster, such as a fire destroying the physical servers. Despite it not being recommended, this solution is outlined below in Figure 3.

Julius Cloos
Security and Risk Management
Tutor: Dr. Siddiqui

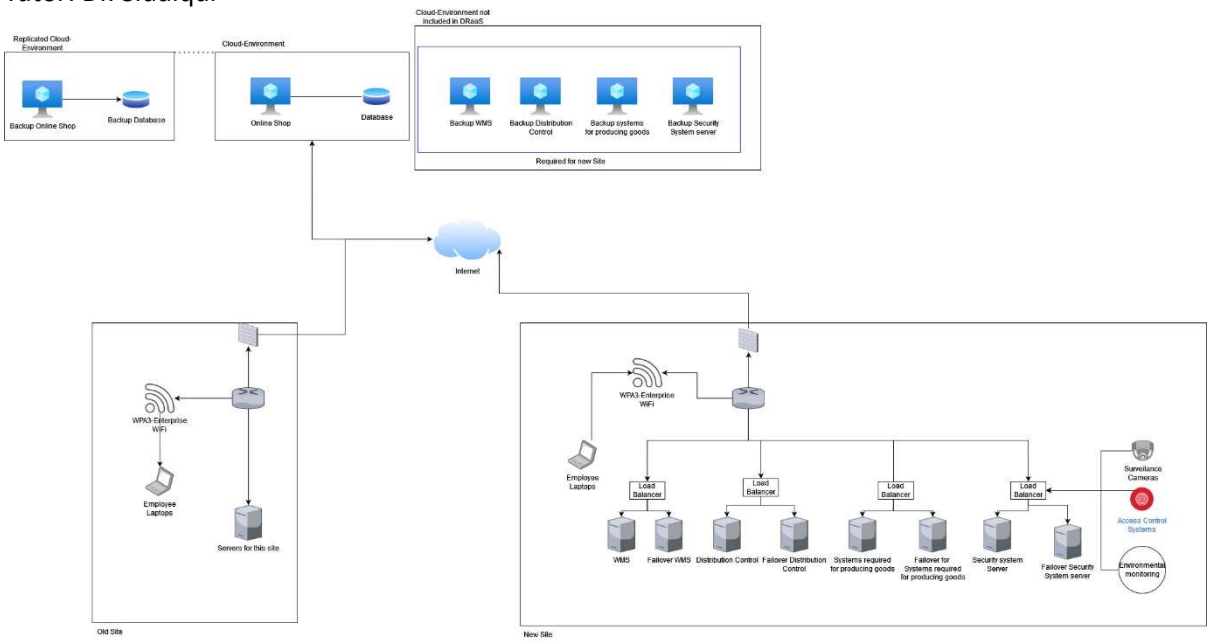

Fig. 3: Diagram showing the infrastructure for disaster recovery, employing fail-over clusters. Created using draw.io.

Solutions such as Microsoft Azure Site Recovery allow for the replication of On-Premise Virtual Machines to the cloud (Microsoft, 2024). To reduce operating cost even more, this report recommends to fully embrace cloud computing and outsource all servers to the cloud, as shown in Figure 4.

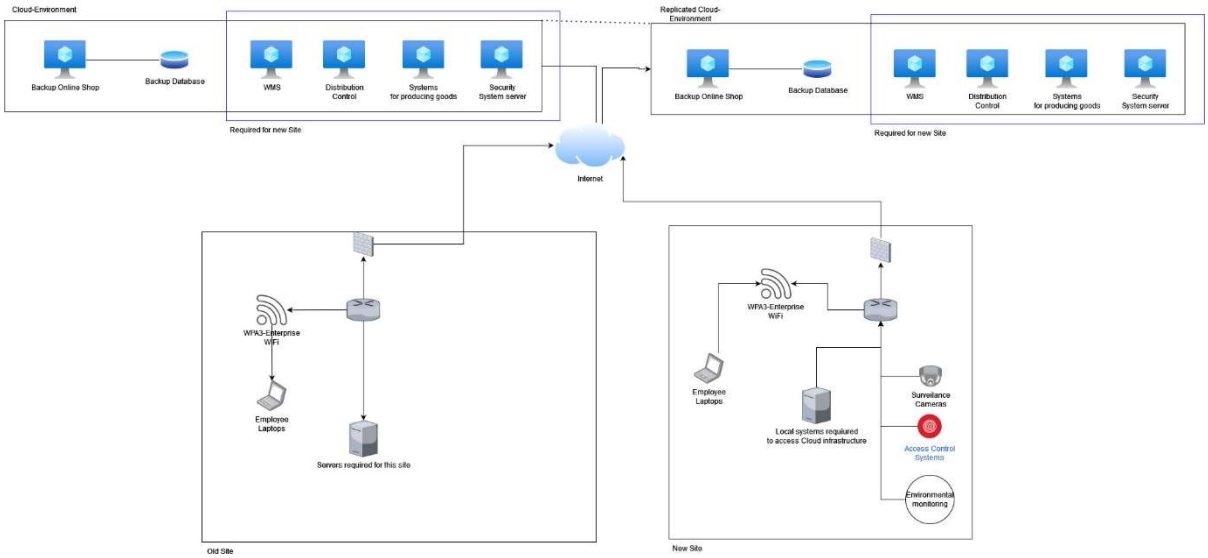

Fig. 4: Diagram showing the infrastructure for disaster recovery, employing cloud-based systems and fully utilizing DRaaS. Created using draw.io.

As of August 2024, Azure Site Recovery is supported for servers in the Europe-region (Microsoft, 2024). This is advantageous due to GDPR requirements requiring businesses to store data on European citizens inside the EU.

Julius Cloos
Security and Risk Management
Tutor: Dr. Siddiqui

Conclusions

In conclusion, Pampered Pets should continue to use its DRaaS provider and integrate the new center into the existing DR strategy, while considering to setup its servers as virtual machines in the cloud to further capitalize on the benefits of cloud computing. However, it must also ensure to abide by the GDPR regulations and, for example, make sure to use cloud providers which provide physical servers in the European Union to avoid having to pay heavy fines.

When Pampered Pets continues to grow its business, perhaps expansions of the existing DR strategy can be considered, further reducing downtime in systems such as the web server by using concepts such as failover clusters as described in Figure 4. However, this should be considered very carefully and only done when necessary, as this not only causes high initial costs for the servers and the changes necessary in the IT infrastructure, but also carries maintenance costs, such as increased workload for the administrators and power costs.

If Pampered Pets requests it, further analysis is possible to outline the detailed technical requirements for the integrated DR strategy, such as including security systems like web application firewalls into the replicated cloud environment.

References

Abualkishik, A. Z., Alwan, A. A., Gulzar, Y. (2020) Disaster Recovery in Cloud Computing Systems: An Overview. *International Journal of Advanced Computer Science and Applications* 11(9): 702-710. Available from: https://thesai.org/Downloads/Volume11No9/Paper_84-Disaster_Recovery_in_Cloud_Computing_Systems.pdf [Accessed 27 July 2024].

Ahmed, N., Jha, S., Kanhere, S., Michelin, R., Kanhere, S. & Seneviratne, A. (2020) 'Leveraging lightweight blockchain to establish data integrity for surveillance cameras', *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).* Toronto, Canada, 3-6 May. 1-3.

Akhtar, N., Dalal, N., Gupta, A., Karamchandani, N., Kasbekar, G., & Parekh, J. (2022) 'A Wireless Intrusion Detection System for 802.11 WPA3 Networks', *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*. Bengaluru, India, 3-8 January. 384-392.

Albin, M., Foroughi, A., Kocakulah, M. (2006) 'Perspectives on Global Supply Chain Supply-Side Risk Management', *2006 Technology Management for the Global Future - PICMET 2006 Conference*. Istanbul, Turkey, 8-13 July. 2732-2740.

Bititci, U. S., Er-Kara & M., Ghadge, A. (2020) Modelling the impact of climate change risk on supply chain performance. *International journal of Production Research*. DOI: http://dx.doi.org/10.2139/ssrn.3652664

Bültmann, L. A. (2022) Backups and the Right to Erasure. Available from: https://www.datenschutz-notizen.de/backups-and-the-right-to-erasure-1434153/ [Accessed 26 July 2024].

Charvériat, C. (2000) Natural Disasters in Latin America and the Caribbean: An Overview of Risk. Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817233 [Accessed 01 August 2024].

Cloudflare (2024) What does 'vendor lock-in' mean?. Available from: https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/ [Accessed 27 July 2024].

Davies, J. (2024) How Does PCI DSS 4.0 Affect Web Application Firewalls?. Available from: https://www.tripwire.com/state-of-security/how-does-pci-dss-40-affect-web-application-firewalls [Accessed 02 August 2024].

French, D.N., Hibbs, A.E., Hodgson, D., Thompson, K.G., Spears, I.R. (2011) Peak and average rectified EMG measures: Which method of data reduction should be used for assessing core training exercises?. *Journal of Electromyography and Kinesiology* 21(1): 102-111. DOI: https://doi.org/10.1016/j.jelekin.2010.06.001

Gimenez, C., Humphreys, P., McIvor, R., Wiengarten, F. (2016) Risk, risk management practices, and the success of supply chain integration. *International Journal of Production Economics* 171(3): 361-370. DOI: https://doi.org/10.1016/j.ijpe.2015.03.020

Grecos, C., Hadhrami, T., Wang, Q. (2012) ‘Real-time visual communication to aid disaster recovery in a multi-segment hybrid wireless networking system’, *2012 SPIE Photonics Europe*. Brussels, Belgium, 16-19 April.

IBM (N.D.) Was ist die Monte-Carlo-Simulation?. Available from: https://www.ibm.com/de-de/topics/monte-carlo-simulation [Accessed 25 July 2024].

InCountry (2024) Navigating GDPR data sovereignty requirements. Available from: https://incountry.com/blog/navigating-gdpr-data-sovereignty-requirements/ [Accessed 28 July 2024].

Microsoft (2024) About Site Recovery. Available from: https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview [Accessed 30 July 2024].

Rudden, J. (2024) Biggest risks to businesses worldwide 2018-2024. Available from: https://www.statista.com/statistics/422171/leading-business-risks-globally/ [Accessed 27 July 2024].

SealMetrics (2024) Location data complying with GDPR. Available from: https://sealmetrics.com/gdpr-location-data-eu/ [Accessed 27 July 2024].

Thahiba, F., Paul, F., Richards, G., G, K., & Pais, S. (2022) Automated Warehouse Control System Design. *International Journal of Advanced Research in Science, Communication and Technology* 2(1): 39-43. DOI: https://doi.org/10.48175/ijarsct-7063

Wolford, B. (2024) What is GDPR, the EU’s new data protection law?. Available from: https://gdpr.eu/what-is-gdpr/ [Accessed 26 July 2024]. (4)