Executive Summary

Risk Modelling and Continuity Strategy for Pampered Pets Digitalisation

Course: MSc in Cybersecurity \ Security and Risk Management

Date: 13/10/2025

Table of Contents

Executive Summary

The move by Pampered Pets to digitalise its operations and venture into international supply chains by opening automated warehouses is a radical but dangerous venture. The inflow of celebrity customers such as His Royal Highness the King and Prince Albert II of Monaco puts even greater strain on the need to maintain the quality of the products and the robustness of the supply chain. This report analyses the likelihood that an alteration in the operations could affect the quality or availability and suggests mitigation strategies with a disaster recovery (DR) plan to ensure business continuity.

The quantitative risk modelling involving Monte Carlo simulations and updating using Bayesian models indicate a 40% chance of disruption of the supply chain, as compared to 35-40% chance of cybersecurity breaches. The quality failure in suppliers is less prevalent at 20 percent with high reputational effects. The risk of warehouse automation is considered to be 15% probability, and the risk of GDPR compliance failure is estimated to be 25 percent. These results underscore the two risks of digital and operational vulnerability.

The categories of recommendations include quality assurance of suppliers, resilience to cybersecurity, business continuity planning, and adherence to the interpretation of the ISO and GDPR standards. It is suggested to implement a multi-cloud active-active with Kubernetes architecture to achieve the high DR requirements i.e. less than one minute downtime and data loss. In general, in the context of maintaining its image and meeting the needs of the premium client segment, Pampered Pets can integrate good governance, online security, and international supply chain management into its transformation process.

Introduction

Pampered Pets has embarked on a big digitalisation discovery, which tries to transform the outdated business model into a new and technological-enhanced business model. This change includes the expansion of online platforms to broaden customer access and the development of global supply chains to extend market presence. Some of these supply chains feature automated warehouses, which are expected to streamline logistics and increase efficiency.

These initiatives provide significant growth, innovation, and competitiveness opportunities in a constantly digitalised market, but they come with new kinds of risks that need to be carefully measured and mitigated by the organisation. Some of the vulnerabilities that expansion into international supply chains exposes the business to are the geopolitical instability, exchange rate fluctuations, and the risk of failure of supplier’s reliability.

Similarly, automated warehouse application is also problematic due to system failures, downtimes, and data corruption. The fact that the company has high profile customers such as His Royal Highness the King and Prince Albert II of Monaco puts the preservation of the globally recognised quality and quantity of products under more pressure. Quantitative risk modelling is used in the report to estimate the likelihood of disruption and describes comprehensive actions that should be employed to remove the risk and restore after a disaster.

Potential Risks to Quality and Supply Chain

The implementation of warehouse automation and international supply chains make the risk profile of the business radically different. A lack of consistency in the suppliers, unstable geopolitical conditions, and currency, as well as the introduction of a logistic

delay are considered supply chain risks (Hammad et al., 2025). Cyber weaknesses in third party suppliers and international logistics providers also lead to an increased vulnerability to disruption (Lin et al., 2025).

Automated warehouses pose the threats of system failure, malfunction of technology and lost data. Even temporary failures can disrupt the order fulfilment and can impact customer satisfaction. These risks revolve around cybersecurity such as ransomware, denial-of-service, and account takeovers, plus ransomware attacks have in recent years hit almost 70 percent of retail companies (Keenan, 2024). Due to the interconnection of digital logistics-based platforms, Pampered Pets is susceptible to cascading failures across the networks (Neethirajan, 2025).

Other possible factors that can impact on the quality of products is through unreliable suppliers or lack of consistency in the raw materials. The concept of blockchain-facilitated monitoring of supply chains has also been cited as an ideal solution in the context of assuring traceability and quality-checking of supply chains within international markets (Gawai, 2025).

Quantitative Risk Modelling

Selection of Modelling Approach

The research paper uses a mixed methodology that involves the Monte Carlo simulations and the Bayesian modelling of probability. Monte Carlo simulations can be used to generate probability distributions of risk events in the face of uncertainty with Bayesian modelling methods being able to update the probabilities as new operations and supply chain evidence is received. This incorporation provides a strong source of uncertainty of digitalisation and globalisation (Neethirajan, 2025).

Assumptions and Data

The model estimates the ransomware risk to be about 35 a year in the case of SMEs that undergo digital transformation (Marks, 2024). The failure of suppliers is pegged at 20, according to the industry standards. Geopolitical shocks are approximated to be 30% in the past, according to historic trade instability (Luo, 2022). The supply chain cybersecurity vulnerabilities are modelled at 40%, which corresponds to the latest results about the third-party attacks (Lin et al., 2025).

Results

The outcomes of the quantitative risk modelling demonstrate evident trends of the weaknesses of Pampered Pets as it continues by expanding its business to digital platforms, global supply chains, and robotic warehouses. Cybersecurity attacks, having a risk of 35-40 percent, were the greatest threat in terms of likelihood and the likelihood of being disrupted. Since the company uses online services to process orders and control their warehouse, these breaches may result in the company coming to a standstill and losing valuable data. The failure of suppliers in quality was identified as less common, and the chance of such failure was 20 percent, but the reputation loss caused by bad quality or inconsistent supplies may be extreme, especially in high-profile clients who require impeccable quality.

Geopolitical or logistical shocks, whether this is through trade or transport delay, or instability in the region, explained a 30-40 likelihood meaning that international dependencies are still a challenge. Less common but high impact, Warehouse automation failures (15) can lead to significant service disruptions due to potential downtime and order backlogs. Lastly, the amount of GDPR compliance failures approximated to 25% as it is still a challenge to safeguard customer data within

digitalised systems. All these findings demonstrate cybersecurity and supply chain risks as the most probable ones, and supplier quality is the most reputationally sensitive.

Risk Category	Probability	Impact Level	Notes
Cybersecurity breaches	35–40%	High	Disruption of systems, data loss
Supplier quality failures	20%	High	Severe reputational consequences
Geopolitical/logistical issues	30–40%	Medium–High	Delays, trade restrictions, costs
Warehouse automation failure	15%	High	Operational downtime, lost orders
GDPR compliance failures	25%	High	Regulatory fines, trust erosion

Summary of Results and Recommendations

According to the quantitative analysis, there is a probability risk of 20% of quality compromise that is mainly associated with supply failure. Measures can involve tracing through the use of blockchain, auditing suppliers and a hybrid sourcing model (Gawai, 2025).

There is a 40 percent chance of supply chain disruptions, which can be affected by the geopolitical instability and the fluctuation of the currency. Some recommendations are to diversify suppliers, maintain strategic stock reserves and use currency hedging. The operational resilience can be enhanced through the application of Industry 4.0 (Hammad et al., 2025).

The highest risk probability is with cybersecurity breaches, which is estimated to be 35-40 percent. Examples of such strategies are multi-factor authentication,

compliance with ISO 27001 standards and active training on phishing (Neethirajan, 2025). Moreover, it is important to extend the policies to include third party vendors.

Business Continuity and Disaster Recovery Strategy

The need of Ms. O'dour to have constant access with a minimum of one minute and at most one minute of inaccessibility, which is a failover time, defines a very high standard of business continuity and disaster recovery planning. In order to do so, an advanced resilience strategy should be adopted. The solution suggested is the multi-cloud active-active configuration, where the workloads would be replicated on the top-tier platforms, which include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud simultaneously. This will help in assuring that in case one of the providers has gone down or hitched, the other will be able to completely take over and continue without service interruptions.

At the same time, database clustering and point-in-time recovery features ensure that the organisation can achieve high Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) and therefore, protect the availability of services and integrity of data. Furthermore, in dealing with the issue of vendor lock-in, the use of containerisation with Kubernetes is recommended. The use of Kubernetes facilitates workload portability between providers so that the company can be flexible, adaptive, and resilient in the long-term infrastructure strategy (Mazabow, 2025). Together, this architecture meets the requirements of continuity in operations, while also makes Pampered Pets a technologically advanced, secure and reliable enterprise.

Compliance and Security Standards

The compliance with GDPR is a strategic necessity of Pampered Pets, especially considering the growth of the business into the global market and the variety of

customers, including high-profile clients. According to the law, personal data must be handled in a legal, transparent and secure manner and therefore it is vital that systems must be designed based on the principle of privacy-by-design. This includes the implementation of security measures such as reduction of data, data storage and default encryption in all operations and electronic processes. The high encryption levels and the 24-hour surveillance systems ensure the confidential customer and transactional information are not abused internally and leaked externally.

The company should integrate the international best practice standards as an extension of the governance, such as the ISO 27001 information security management and ISO 22301 business continuity management. These standards could offer structured methods for analysing risks, managing them, and improving resilience to both cyber and physical attacks. Besides compliance, supply chain transparency has also become an increasing pressure among consumers across the borders. Technological solutions such as tracking system based on a blockchain helps to enhance tracking of suppliers and logistics partners and guarantees purity of products and customer trust (Gawai, 2025). All these will provide not just legal protection, but reputational power as well, which will help to level Pampered Pets with global ethical and business practices.

Recommendations in Order of Priority

The risk and mitigation plan shows that the activities should be prioritised in terms of the likelihood of their occurrence and their potential damage to the reputation and work of Pampered Pets. The number one priority is supplier quality assurance since high profile clients such as His Royal Highness the King and Prince Albert II of Monaco will not accept inconsistency and unreliability on issues related to product standards. To

boost this sector, it is necessary to introduce supplier audits, contractual quality standards, as well as blockchain-based traceability to maintain transparency in the supply chain.

Cybersecurity reinforcement, which deals with the 35-40-percent likelihood of attack, is the second priority. This involves applying ISO 27001 controls, improving network monitoring, and extending security policies to third-party vendors. Since operations have a global scope, cybersecurity should not be a one-time investment, but a process that is continuous in nature.

The third concern is the disaster recovery (DR) strategy, which is to be developed to ensure the continuation of service and the high level of availability. The next step is the incorporation of GDPR and ISO compliance within all governance structures, which would mean that it is legal and ethical. Lastly, the supply chain has to be diversified to minimise reliance on one area or even one supplier to avoid geopolitical unrest and financial fluctuations.

Conclusion

Pampered Pets' digital transformation represents a pivotal moment in the company's growth, enabling it to harness the advantages of e-commerce, international supply chains, and automated warehouses to deliver efficiency and scalability. Nevertheless, they are also accompanied by major risks that have to be effectively controlled to protect the reputation of the company and its stable performance. Quantitative modelling performed in this report identifies disruptions in supply chains and breaches of cybersecurity as the most likely threats, although supply quality failures are less common but pose the most reputational risk, especially when dealing with high-profile clients and high-quality standards are required.

In order to deal with these threats, it is essential to implement a multi-layered approach. Managing a supply chain using a blockchain-powered monitoring system guarantees supply chain visibility and trust in global sourcing, and hardened cybersecurity architectures based on ISO 27001 offer a defence against cybercrime. Moreover, the introduction of a solid disaster recovery system will ensure to continue serving, despite unfavourable circumstances. All of these actions will not only help to prevent disruption but also build a strong relationship with foreign allies and high-end customers. Consequently, with these protective measures in place, Pampered Pets will be able to establish itself as a safe, eco-friendly, technologically enhanced industry leader in the pet care market, which will guarantee its success in the long term.

References

Boling, B., 2025. *" When Told A Story, They Listen": The Foxfire Magazine's Storytelling Ecology* (Doctoral dissertation, University of Cincinnati).

Eddy, E.P., 2025. *Keep the Girls Shaking: Preserving Occupational Knowledge at the Burlesque Hall of Fame Museum* (Doctoral dissertation, Indiana University).

Gawai, A.S., 2025. *On the blockchain adoption in fisheries and aquaculture supply chains: an empirical study on Indian stakeholders' perceptions and the US consumer preferences for blockchain-enabled shrimp supply chain* (Doctoral dissertation, University of Reading).

Hammad, M., Panaousis, M., Ali, H. and Khan, W.A., 2025. Smart Manufacturing in Food and Beverage Industry. In *Smart Manufacturing Blueprint: Navigating Industry 4.0 Across Diverse Sectors* (pp. 213-243). Cham: Springer Nature Switzerland.

Lin, L.S., Mekonnen, G., Aslett, D. and Allan, D., 2025, September. Organised Crime and Regional Political Dynamics: Examining Factors Driving Chinese Telecom Fraud

in Southeast Asia. In *25th Annual Conference of the European Society of Criminology: EUROCRIM 2025*.

Mazabow, S., 2025. *Waste to Paste: Sustainable and Circular Novel Material Composites for Explorative Prototyping in Product Design Practice* (Doctoral dissertation, University of Technology Sydney (Australia)).

Neethirajan, S., 2025. Safeguarding digital livestock farming-a comprehensive cybersecurity roadmap for dairy and poultry industries. *Frontiers in Big Data*, *8*, p.1556157.

Sharma, R., 2025. Lifelong pregnancies & rivers adrift: exploring the liminality of the immigrant home in Jhumpa Lahiri's The Namesake and Monica Ali's Brick Lane.