MATTEO MARCHI
ENTERPRISE IT MANAGEMENT MSc
Individual Project: Executive Summary

14/10/2024

Potential Risks to Quality and Supply Chain for Pampered Pets

Pampered Pets' transition to an international supply chain and automated warehouses introduces several risks that could potentially affect both the quality of its products and the security of its supply chain. To analyse these risks effectively, a quantitative risk modelling approach is selected to estimate the likelihood of occurrence and potential impact.

Potential Risks to Product Quality and Supply Chain

Product Quality Risks

- Risk of Quality Degradation from International Suppliers: The variability in ingredient quality, differing regulations, and longer supply lines can affect product consistency.
  (Zhou, Z. and Johnson, M., 2014).
- Risk of Automation errors in Warehousing: Mistakes in automated sorting, storing, and handling processes could lead to incorrect storage conditions, contamination, or spoilage.
- Cybersecurity Risks: Vulnerabilities in automated systems could be exploited, leading to system malfunctions that affect product handling or allow unauthorized access to sensitive data.

Supply Chain Risks

- Supply Chain Disruption Due to Global Instability: Political events, trade wars, or natural disasters in supplier countries could lead to ingredient shortages or delays.
- Logistics and Transportation Delays: Shipping delays or disruptions due to global logistics issues (e.g., port closures, customs delays) could affect product availability.
- Increased Dependency on Technology: Reliance on automated warehouses introduces risks of system malfunctions, breakdowns, or cyberattacks that could halt operations.
  (Paul, S.K., Asian, S., Goh, M. *et al., 2019)*

Quantitative Risk Modelling Approaches

Chosen Models

For Pampered Pets, I've chosen the following quantitative risk modelling approaches to assess the identified risks:

Monte Carlo Simulation (Kumar et al., 2014).

Justification: Monte Carlo simulations are ideal for handling uncertainties in inputs (e.g., supplier reliability, logistics delays) and calculating the range of possible

outcomes. This approach helps to model the variability in product quality and supply chain disruptions.
Application: Used to assess the likelihood of delays and quality degradation by simulating a wide range of scenarios with varying input parameters.

Fault Tree Analysis (FTA) (Bhardwaj & Agrawal, 2022)
Justification: FTA provides a structured method for identifying the root causes of failures in the supply chain and warehousing systems. It breaks down complex systems into their individual components and calculates the probability of overall failure.
Application: Used to model the likelihood of system failures in the automated warehouses or logistics network, with a focus on cybersecurity and system malfunctions.

Monte Carlo Simulation (for Supply Chain and Quality Risks)
Key Assumptions:

- **Supplier Reliability**: The reliability of international suppliers is assumed to range between 80% to 95%, based on historical data from similar industries.
- **Logistics Delays**: Shipping delays are modelled as a probability distribution, with delays typically occurring 10%-15% of the time, increasing during geopolitical or economic instability.
- **Ingredient Quality**: International suppliers may have a 5%-10% lower quality standard than local suppliers, impacting product consistency.

Data Sources:

- Supplier reliability data is based on public reports from the global pet food industry.
- Transportation delay probabilities are estimated using global shipping statistics.
- Internal records on quality checks from Pampered Pets' current local suppliers serve as a baseline for comparison.

Simulation Setup:

- Run 10,000 simulations over a period of 1 year.
- Inputs: Supplier reliability, shipping delay probabilities, and ingredient quality.
- Output: Probability distributions of quality degradation and supply chain disruptions.

Results:

- **Probability of Product Quality Degradation**: 25% chance of a noticeable quality drop due to international suppliers, with the greatest risk during the initial 6 months of the transition.
- **Probability of Supply Chain Disruption**: 35% chance of significant supply chain disruption at least once within the next year.

Fault Tree Analysis (for Automation and Cybersecurity Risks)
Key Assumptions:

- **System Failure Rates**: Automation systems in warehouses are assumed to have a failure rate of 1% per month due to either hardware or software issues.
- **Cybersecurity Breaches**: Likelihood of a successful cyberattack is modelled at 2%-3% annually, assuming industry-standard security measures are in place.

Data Sources:

- Industry reports on automation system reliability and cybersecurity incidents in similar-sized businesses are used to estimate failure rates.

Calculation:

- FTA is constructed with the following top-level failures:
  - **Warehouse System Failure**: Composed of potential hardware, software, and communication failures.
  - **Cybersecurity Breach**: Modelled with probabilities for system vulnerabilities and potential exploitation by external actors.

Results:

- **Overall Probability of System Failure**: 12% annually, with a higher likelihood of issues stemming from software updates or improper configuration.
- **Cybersecurity Risk**: 2%-3% probability annually of a significant cyber breach that could lead to product delays or system downtime.

Results of Quantitative Models

Risk Type	Probability
Product Quality Degradation	25% (Monte Carlo)
Supply Chain Disruption	35% (Monte Carlo)
Automation System Failure	12% (Fault Tree Analysis)
Cybersecurity Breach	2%-3% (Fault Tree Analysis)

The quantitative models indicate moderate to high probabilities of risks affecting both product quality and the supply chain as Pampered Pets transitions to an international model. Supply chain disruptions present the highest risk, with a 35% likelihood, while product quality degradation due to international suppliers poses a 25% risk.
To mitigate these risks, Pampered Pets should focus on supplier vetting, system monitoring, and cybersecurity enhancements while continuing to analyse and update risk models as the company grows and the supply chain becomes more complex.

Summary of Quantitative Modelling Results and Recommendations for Pampered Pets

Risk of Quality Loss

Results:

- **Probability of Quality Degradation**:
  - Estimated at 25% over the first year due to the introduction of international suppliers.
  - Main risks include variability in ingredient quality standards, lack of immediate oversight compared to local suppliers, and the potential for longer supply chains to impact ingredient freshness or integrity.

Recommendations:

- Supplier Vetting: Implement a rigorous supplier vetting process that includes detailed inspections, adherence to quality standards, and certifications. Ensure all international suppliers meet or exceed current local supplier standards.

- Quality Audits: Perform random sampling and third-party audits on the quality of ingredients sourced from international suppliers to ensure consistent standards are met.
- In-House Production Oversight: Maintain oversight on in-house processing, ensuring strict adherence to quality control protocols for packing and ingredient handling, even with automated systems.

Risk of Supply Chain Issues
Results:

- **Probability of Supply Chain Disruption**:
    - Estimated at 35% over the next year. This is the highest risk identified, particularly during the transition to an international supply chain.
    - Key risks include:
        - **Logistics and Transportation Delays** (15%-20% chance): Due to **customs regulations, port delays**, or global shipping challenges, especially with the ongoing volatility in international trade.
        - **Supplier Failure or Delay** (10%-15% chance): Political instability, regulatory differences, or **natural disasters** affecting suppliers in different countries.
        - **Automation and Technology Malfunctions** (12% chance): Failures in automated warehousing systems, including software glitches, system breakdowns, or cybersecurity incidents.

(Willis Towers Watson, 2023)
Possible solutions:

- Supplier Diversification: Avoid reliance on a single international supplier or region. By sourcing from multiple suppliers in different regions, Pampered Pets can reduce the risk of supplier failure and create a buffer against regional disruptions.
- Buffer Stock and Local Warehousing: Build buffer stock at critical automated warehouses to cushion against potential logistics delays or supply shortages. Additionally, consider maintaining local sourcing for emergency supplies.
- Real-Time Monitoring and Contingency Planning: Implement real-time monitoring systems that provide visibility into the supply chain from sourcing to delivery. This will enable quicker identification of disruptions. Develop contingency plans that outline alternate suppliers or emergency response strategies in case of prolonged delays.
- Cybersecurity Fortification: Strengthen cybersecurity defences to protect against cyberattacks that could cripple automated systems or cause delays in supply chain operations. Regularly audit and update systems to protect against vulnerabilities.

(BCI, 2023)

Summary of Probabilities and Potential Issues

Potential Supply Chain Issues	Probability of Occurrence	Risk Description
Logistics and Transportation Delays	15%-20%	Shipping delays due to customs, port issues, or global trade instability.

Potential Supply Chain Issues	Probability of Occurrence	Risk Description
Supplier Failure or Delay	10%-15%	Disruptions from political instability, regulatory issues, or natural disasters.
Automation System Failure	12%	Software or hardware malfunctions in automated warehouses, causing distribution delays.
Cybersecurity Breach	2%-3%	Potential cyberattacks that could disrupt automated warehouse systems or expose sensitive data.

Recommendations Based on Quantitative Modelling
Based on the risks identified, the following actions are recommended:

1. **Quality Risk Management**:
    - Invest in quality assurance processes for international suppliers.
    - Regular audits and oversight of both international and in-house processes to maintain product consistency.
2. **Supply Chain Resilience**:
    - Diversify suppliers to avoid over-reliance on a single source and mitigate geographic risks.
    - Build buffer stocks and maintain emergency sourcing strategies for critical ingredients.
    - Enhance real-time monitoring of logistics to quickly respond to any emerging issues.
3. **System and Cybersecurity Enhancements**:
    - Focus on system reliability for automated warehousing by conducting routine maintenance and performance checks.
    - Implement strong cybersecurity protocols to defend against potential system breaches or malware attacks.

Disaster Recovery (DR) Solution for Pampered Pets' Online Shop
Ms. O'Dour has outlined stringent requirements for the business continuity and disaster recovery (DR) strategy, specifically:

- 24/7/365 availability of the online shop.
- Less than 1-minute failover to a disaster recovery environment.
- Data loss tolerance: No more than 1 minute of lost data (Recovery Point Objective or RPO).

To meet these requirements, a high-availability architecture with real-time replication is necessary, along with a DR solution that can switch seamlessly in the event of an incident.

DR Solution Design
An active-active DR architecture involves running two or more identical environments (production and DR), with both actively replicating data in real-time. This ensures that if

the primary environment fails, the secondary (DR) environment is instantly available, with minimal downtime and data loss.
Key Components:

- Primary Environment: Runs the online shop during normal operations.
- Secondary Environment (DR): A mirrored environment located in a different region or data center.
- Real-Time Replication: Continuous data replication between the primary and secondary environments ensures that data is always up to date.

Advantages:

- Failover time is minimized to under 1 minute, meeting the Recovery Time Objective (RTO).
- Data loss is minimized to less than 1 minute, aligning with the RPO requirement.
- The solution is resilient to regional outages and infrastructure failures.

Load Balancing and Automatic Failover
To support seamless changeover in the event of a disaster, load balancers are implemented to distribute traffic between the active sites. These load balancers detect failure in the primary environment and automatically redirect traffic to the DR environment.

- Global Load Balancers: Monitor the health of the online shop and switch traffic to the DR environment in case of failure.
- Automatic Failover: Ensures that the switch occurs within seconds, maintaining the required uptime.

Hosting Platform Recommendation
For a robust and scalable DR solution, the following cloud platforms are recommended:
Amazon Web Services (AWS)
AWS offers multi-region redundancy, ensuring that the DR environment is located far enough from the primary environment to be unaffected by regional disasters. AWS also supports real-time data replication and automatic failover with Route 53.
Microsoft Azure
Azure provides similar multi-region capabilities, real-time replication, and automatic failover options.
Google Cloud Platform (GCP)
GCP also offers a high-availability setup with cross-region redundancy and automated failover capabilities.

To minimize Vendor lock-in this risk, Pampered Pets should consider the following
Multi-Cloud Strategy:
Rather than fully relying on one vendor, a multi-cloud approach allows the company to spread infrastructure across multiple platforms (e.g., AWS for primary and Azure for DR).
This reduces dependency on any single vendor and improves resilience.
Use of Open-Source Tools:
Utilize open-source tools for critical components like load balancing, data replication, and monitoring.

Open-source tools are portable across cloud providers, which makes it easier to migrate in the future if needed.

Cross-Cloud Compatibility:

Ensure that the application architecture is cloud-agnostic by using widely supported services such as containerization (Docker, Kubernetes) and API-based architectures. This makes migration to a different cloud provider easier in case vendor lock-in becomes a concern.

(Kumar, I., 2020)

Mitigations for GDPR Compliance (Amoo et al, 2024).

Data Encryption:

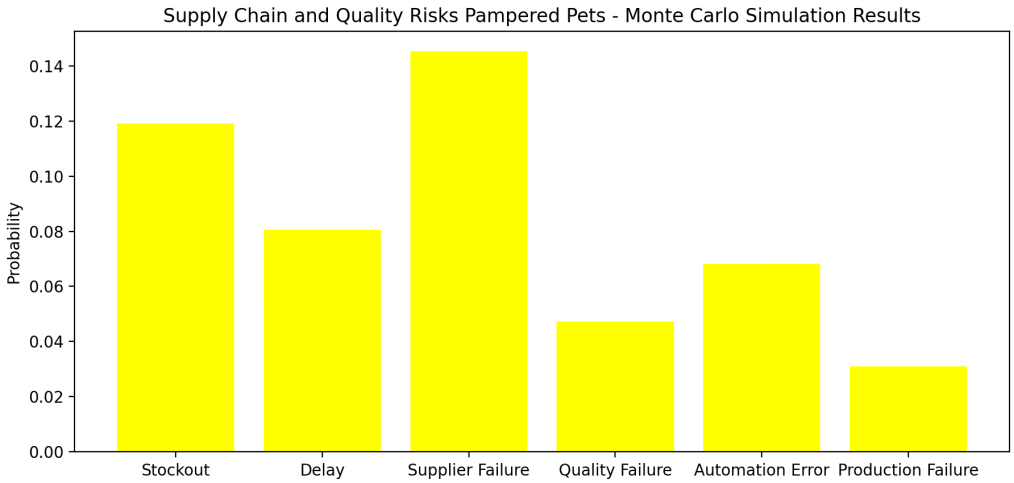
All customer data (personal details, order information, etc.) must be encrypted both during storage (at rest) and transmission (in transit). This protects sensitive data from unauthorized access.

Access Control and Auditing:

Enforce strict access control policies to limit who within the organisation can access customer data. Implement auditing mechanisms to log who accesses or modifies the data.

Data Retention Policies:

Define and enforce a data retention policy that outlines how long customer data is stored and when it will be deleted, in accordance with GDPR's data minimization principles.



Zhou, Z. and Johnson, M. (2014). Quality risk ratings in global supply chains. Production and Operations Management, 23(12), 2152-2162. https://doi.org/10.1111/poms.12251

Paul, S.K., Asian, S., Goh, M. *et al*. Managing sudden transportation disruptions in supply chains under delivery delay and quantity loss. *Ann Oper Res* **273**, 783–814 (2019). https://doi.org/10.1007/s10479-017-2684-z

Kumar, S., Tiffany, M., & Vaidya, S. (2014). Supply chain analysis of e-tailing versus retailing operation – a case study. Enterprise Information Systems, 10(6), 639-665. https://doi.org/10.1080/17517575.2014.986218

Bhardwaj, M. and Agrawal, R. (2022). Benchmarking the failure assessment of perishable product supply chain using fault tree approach: insights from apple case study of india. Benchmarking: An International Journal, 29(10), 3226-3250. https://doi.org/10.1108/bij-08-2021-0465

Willis Towers Watson. (2023). *2023 Global Supply Chain Risk Report*. [online] Available at: https://www.wtwco.com/en-US/insights/2023/02/2023-global-supply-chain-risk-report.

BCI (2023). *BCI Supply Chain Resilience Report 2023*. [online] www.thebci.org. Available at: https://www.thebci.org/resource/bci-supply-chain-resilience-report-2023.html

Kumar, I. (2020). Cloud computing-based disaster recovery. Turkish Journal of Computer and Mathematics Education (Turcomat), 11(1), 815-820. https://doi.org/10.17762/turcomat.v11i1.13562

(2023). Cloud-based business continuity and disaster recovery strategies. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets46236

Olukunle Oladipupo Amoo, Akoh Atadoga, Femi Osasona, Temitayo Oluwaseun Abrahams, Benjamin Samson Ayinla, & Oluwatoyin Ajoke Farayola (2024). Gdpr's impact on cybersecurity: a review focusing on usa and european practices. International Journal of Science and Research Archive, 11(1), 1338-1347. https://doi.org/10.30574/ijsra.2024.11.1.0220