Pampered Pets Risk Assessment - Current Business Operations

Group 1 first draft

I. Introduction

- Brief overview of Pampered Pets and its business operations.
- Importance of conducting a risk assessment for current operations.

Potential references

- Sharma, J., Tyagi, M. and Kazançoğlu, Y., 2024. Impact of digital technologies on the risk assessment in the food supply chain: a wake towards digitalisation. International Journal of Food Science & Technology.
- Mostaghel, R., Oghazi, P., Parida, V. and Sohrabpour, V., 2022. Digitalization driven retail business model innovation: Evaluation of past and avenues for future research trends. Journal of Business Research, 146, pp.134-145.
- Malenkov, Y., Kapustina, I., Kudryavtseva, G., Shishkin, V.V. and Shishkin, V.I., 2021. Digitalization and strategic transformation of retail chain stores: Trends, impacts, prospects. Journal of Open Innovation: Technology, Market, and Complexity, 7(2), p.108.

Content

Pampered pets is a customer-centric business focussed on the quality of their products, and specialists in face-to-face service. They have made attempts to incorporate technology into their value chain, and this assessment will begin by outlining the current risks involved in the business model and recommended mitigation strategies. Secondly, we will suggest further technology implementation, and consider the associated risks of doing so. Many organisations find risk management challenging (Barafort et al., 2018), but

References

Béatrix Barafort, Antoni-Lluís Mesquida, Antònia Mas,

Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context,

Computer Standards & Interfaces,

Volume 60,

2018,

Pages 57-66,

ISSN 0920-5489,

https://doi.org/10.1016/j.csi.2018.04.010.

II. Methodology Selection

- Justification for selecting a specific risk assessment methodology (likely focussed on qualitative, but incorporating elements of quantitative).
- Explanation of how the chosen methodology aligns with the business context and objectives.

Potential references

- Kovaitė and Stankevičienė, 2019
- Landoll, D., 2021. The security risk assessment handbook: A complete guide for performing security risk assessments. CRC press.
- Piroth, P., Rüger-Muck, E. and Bruwer, J., 2020. Digitalisation in grocery retailing in Germany: an exploratory study. The International Review of Retail, Distribution and Consumer Research, 30(5), pp.479-497.

Content

Propose the use of semi-quantitative, as qualitative may be difficult to compare with a full quantitative review in section 2. This takes the benefits of qualitative but applies a more numerical scale to the process. Ie using 1-100 or 1-10 as opposed to high medium low, and then a comparison can be made.

"Perhaps the easiest application of multiple criteria analysis is the simple multiattribute rating theory (SMART). SMART provides decision makers with a means to identify the relative importance of criteria in terms of weights, and measures the relative performance of each alternative on each criterion in terms of scores. In this application, we will include criteria of seven factors: Customer service; Reliability and scalability, Availability, Integration; Financial factors; Security; and Service level monitoring & management." - Olson, D.L. & Desheng D.W. (2020) Enterprise Risk Management Models (3rd edition)...

- The above may be useful as SMART seems to link qualitative to quantitative well.

Big emphasis on **selection** of risk methodology and modelling. Discuss frameworks and justify with sources. (NIST, ISO27001, PCIDSS) (EG. Assets - customer data, Risk/threat - malware, vulnerabilities - lack of encryption, impact - customer data stolen, Rating, mitigations - using encryption) (Quantitative, qualitative, hybrid)

III. Current Business Operations Overview

- Description of Pampered Pets' current business model and operations.
- Highlight key aspects such as staff roles, customer interactions, IT infrastructure, and data handling processes.

Potential references

- Haas, Y., 2019. Developing a generic retail business model–a qualitative comparative study. International Journal of Retail & Distribution Management, 47(10), pp.1029-1056.

Content

- Business core values
    - Focus on quality of pet food
    - Local ingredients, items prepared and packed in house

- Current IT Assets

Asset	Use
Email system	Small portion of customer orders, staff reply with email when order is ready
Old, networked computer	Spreadsheets used to keep track of stock and item locations.
Point of sale computer	Digital record of transactions, sales, purchases for VAT and tax purposes
Wireless gateway and hub	Both computers are connected as well as staff personal devices for work use

- Key Stakeholders

Name	Role
Alice	Owner/manager
Cathy	Shop manager
Orla	Investor (Sponsor)
Andrea	Store assistant
Harry	Warehouse manager

IV. Risk Identification

- Internal Threats and Risks:
    - Identification of potential risks stemming from within the organization, such as human error, negligence, or insider threats.
    - NIST SP 800-30, ISO 27005?
- External Threats and Risks:
    - Identification of external threats and risks, including cyber threats, supply chain vulnerabilities, and physical security risks.

- - STRIDE? CRAMM? DREAD?
  - Impact Assessment:
    - Evaluation of the potential impact of identified risks on business operations, including financial, reputational, and operational impacts.
  - Likelihood Assessment:
    - Assessment of the likelihood of each identified risk occurring, considering historical data, industry trends, and threat intelligence.

Potential references

- Anderson, R. (2020) Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Indianapolis: Wiley Publishing.
- NCSC (National Cyber Security Centre) (2023) Risk Management - Threat Modelling https://www.ncsc.gov.uk/collection/risk-management/threat-modelling
- Sharmaa, A., Jain, R. and Pajni, N.S., 2022. Risk Identification Techniques in Retail Industry: A case study of Tesco Plc. J. Corp. Gov. Insur. Risk Manag, 9, pp.201-214.
- Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

- Kovaitė and Stankevičienė, 2019

Risk types - technical, competence, behavioural, data security, financial

Content

Asset	Vulnerabilities	Impact	Likelihood	Type
Email order system	Man in the middle attacks, spam mail, trojan horse			Data security
Old networked computer	Out of date operating system, unsupported software, corruption, loss			Data security, technical

	of information			
Spreadsheet package	Tracking, version control, usability in case of other user			Technical, competence
Point of sale computer	Payment security, tax evidence			

PASTA

1. Define objectives

Business Objectives

Primary objective: To serve high-quality pet food.

Secondary objectives: To provide the best possible customer experience; to maintain a reliable local supply chain.

Security & Compliance Requirements

Handling of customer data must follow GDPR; processing of payment information must follow PCI-DSS; VAT and tax records must be properly maintained to comply with UK law; food preparation and storage must comply with food standards agency; all food labelling must comply with regulation; The Animal Feed (Composition, Marketing and Use) (England) Regulations 2015.

2. Define Technical Schope
3. Application Decomposition
4. Threat Analysis
5. Vulnerability & Weakness Analysis
6. Attack Modelling
7. Risk & Impact Analysis

V. Mitigation Strategies

- Internal Controls:
    - Proposals for implementing internal controls to mitigate internal risks, such as staff training, access controls, and regular audits.
- External Controls:
    - Suggestions for implementing external controls to mitigate external risks, such as cybersecurity measures, vendor management practices, and physical security measures.
- Identification of high-priority risks based on their severity and likelihood.
- Recommendation of mitigation measures based on their effectiveness and feasibility.

Potential references

- Sharif, M.H.U. and Datta, R., 2020. Risk Management for a Retail Business. Retrieved from URL: https://www. researchgate. net/profile/Md_Haris_Sharif/publicatio n/342212234_Risk_Management_for_a_Retail_Business/links/5 ee8ebaa458515814a62e3fa/Risk-Management-for-a-Retail-Business. Pdf.
- Lambrinoudakis et al (2022) COMPENDIUM OF RISK MANAGEMENT FRAMEWORKS WITH POTENTIAL INTEROPERABILITY. Available from: https://www.enisa.europa.eu/publications/compendium-of-risk-managementfra meworks/@@download/fullReport doi:10.2824/75906

VI. Summary and Recommendations

- Summary of key findings from the risk assessment.
- Clear recommendations for mitigating identified risks and enhancing the security posture of Pampered Pets' current operations.

Potential references

- Weyer, J., Tiberius, V., Bican, P. & Kraus, S. (2020) Digitizing grocery retailing: The role of emerging technologies in the value chain. *International Journal of Innovation and Technology Management* 17(08): 2050058.

VII. Conclusion

- Recap of the importance of conducting regular risk assessments for maintaining cybersecurity resilience.
- Call to action for implementing the recommended mitigation measures.

VIII. References