Development Team Project: Risk Identification Report For Pampered Pets

SRM_PCOM7E

BY

NJIDEKA OZOEMENA & BLESSING

MONSI (GROUP 3)

September 2023

Introduction

For the Risk Assessment Methodology for Pampered Pets(PP) checklists 1 and 2, we are employing the following frameworks: NIST 800-181 Business Impact Analysis (BIA), Qualitative Risk Assessment, ISO 27001, Payment Card Industry Data Security Standard (PCI DSS), GDPR (for European data processing), STRIDE, and Risk Assessment Matrix. The proposed risk rating is subject to adjustment based on the client's risk appetite. Our presentation word count is 1,093.

Justification:

We are employing a Qualitative Risk Assessment to identify risks and threats in PP's current business model, with a focus on financial and technical factors. This approach is backed by STRIDE threat modeling and Risk Assessment Matrix (RAM) for threat identification, mitigation, and risk impact prioritisation (Shostack, A. 2014).

NIST 800-181 BIA Framework analyses Financial, Reputation, Regulatory, Social, Production output, and Environmental risks' impact (Orbussoftware, N.D.).

ISO 27001 will safeguard sensitive data related to sales, inventory, logistics, and taxes post-digitalisation (Lecturecast 3).

PCI DSS compliance is necessary for handling credit/debit card information (BigCommerce, N.D.).

RISK IDENTIFICATION AND MITIGATION OF CURRENT BUSINESS MODEL OF PP

Asset	Risk/ Threat	Impact	Rating	Mitigation

Wireless Gateway & Hub	➔ Denial of Service (DoS) ➔ Information Disclosure (Hub Broadcast Issues) ➔ Physical Security Risk (Rogue Access Point) ➔ MAC Address Spoofing ➔ Lack of Hub Segmentation ➔ Data Snooping ➔ Lack of Security Features	➔ Network Flooding ➔ Network Performance Degradation and Data Exposure ➔ Mail Traffic Diversion by Threat Actors ➔ Data Privacy Breaches ➔ Loss of Sales ➔ Sensitive Information Disclosure and Data Theft	High	➔ Implement switches and firewalls. ➔ Utilise strong passwords, WPA3 encryption, and MAC filtering (NIST 800-97). ➔ Implement data encryption and use VPN ➔ Enforce authentication messaging policy (SPF & DMARC). ➔ Implement Antivirus, Intrusion

				Detection/Prevention systems. ➔ Physical device Access controls. ➔ Active network monitoring.

Hardware (Old Computer) & Software Application	➔ Security vulnerabilities (malware and virus infections) ➔ Data breaches. ➔ Reduced productivity. ➔ Downtime and unreliability.	➔ Exploitation of unpatched vulnerabilities. ➔ Slow old computers affect productivity. ➔ Incompatibility with modern software. ➔ System crashes leading to data loss and regulatory issues. ➔ Data breach:	High	➔ Change old computer to newer version. ➔ Installation antivirus and anti-malware. ➔ Implement Hardware/Data back-up solution and recovery mechanism. ➔ Deprovision of old applications. ➔ Encrypt sensitive data.

		leads to reputation damage and legal liabilities.		
Employees	➔ Information Disclosure ➔ Elevation of privilege ➔ Inefficient Processes ➔ Weak Passwords ➔ Phishing/Vishing Attacks	➔ Unauthorised access, data loss/theft ➔ Confidentiality breaches, legal consequences ➔ Social Engineering incidents. ➔ Employee becomes a competitor (with access to both	Medium	➔ Implement adequate Access control. ➔ Security Awareness Training. ➔ Employees' monitoring and behaviour analytics solution to detect unusual/ suspicious activities. ➔ Limit access

		suppliers and buyers) ➔ Theft of raw materials by employees'		to the supplier and other business trade secrets.

Adhering to ISO270001(ISMS) guidelines will provide further mitigation to the current challenges faced by PP.

Checklist 2:

Below are the proposed changes to achieve Pampered Pet's Digitalisation Business Model following the Industry 4.0 revolution.

- Upgrade PP Warehouse Management System (e.g. Oracle Warehouse Management Cloud).
- E-commerce Platform.
- Mobile Application.
- Data Backup and Recovery (Implementation of a Business Continuity Plan (BCP) and Data Recovery Plan (DRP)).

- Pro-active Employee Training and security best practice awareness. (SANS 2022)
- Digital Payments Infrastructure (payment gateway and APIs).

Risk and Threat Modeling Exercise

T**hreat profiling using STRIDE for Digitlised Pampered Pet**

Spoofing: Unauthorised access to customers' accounts and phishing emails to employees.

Tampering: Unauthorised changes to inventory records or alteration of data and software configurations.

Repudiation: Customers deny placing orders or lack audit trails to prove who accessed or modified data in the cloud.

Information Disclosure: Misconfigured cloud storage settings leading to data exposure.

Denial of Service: Disruption of online services or resource exhaustion in a virtualised environment.

Elevation of Privilege: Unauthorised access to admin functions.

RISK ASSESSMENT OF PP PROPOSED DIGITALISED BUSINESS MODEL

Key Areas	Risk Description	Event (Threat)	Impact (Business effect)	Risk Rating
DATA/CUSTOMER LIFECYCLE/	Data Governance	➔ Poor Data lifecycle ➔ Customer Negligence ➔ Lack of proper classification	➔ Financial loss ➔ Data exfiltration ➔ PII exposure	Low
DATA/ ASSET	Disaster Recovery	➔ Unplanned outage ➔ Hosting issues	➔ Unavailability of pampered website ➔ Network Downtime	Medium
DATA/ ASSET/EMPLOYEE/ CUSTOMER LIFECYCLE/	Access Risk	➔ Deletion of data by staff ➔ Technical issues ➔ Malicious employee	➔ Data loss ➔ Availability issues ➔ Stolen data or proprietary information ➔ Application/Websi	Medium

		➔ Poor employee lifecycle ➔ System breach ➔ DDoS ➔ Virus/malware on systems	te unavailability.	
ASSET	Technology	➔ Technological failures ➔ Scalability, ➔ Compatibility and accuracy of the functionality of the implemented technology (Deloitte, 2018)	➔ Potential losses (financial, data, time)	Medium
ASSET/DAT	Cyber	➔ Payment	➔ Identity theft	Medium

A		gateway account takeover. ➔ Unauthorised access usage ➔ Delayed vulnerability management ➔ Poor network architecture ➔ Eavesdropping	➔ Ransomware ➔ Malware	
ASSET	Asset lifecycle	➔ Unplanned and Planned maintenance ➔ Fire in the office ➔ Vulnerable API or third-party plugin ➔ Loss of	➔ Unavailability ➔ Inability to use office ➔ Remote code execution (RCE) ➔ Data leakage	Medium

		laptop		
DATA	Privacy	➔ PII exposure ➔ Cross border data	➔ Problems with data transfer regulations. ➔ Problems with data classification leading to sensitive data exposure.	High
ASSET	Manage security incidents and natural disasters	➔ Lack of adequate incidence response plan, BCP and DRP ➔ Inadequate control in operation	➔ Breach of critical system. ➔ Inability to continue business operation	Medium
DATA	Legal & regulatory compliance	➔ None or partial compliance	➔ Fines ➔ Lost of business reputation	Low

		issues	➔ Financial loss	
DATA/ASSET	Third-party data compliance risks	➔ Data breach ➔ Accidental data leakage	➔ Law-suits from customer	Medium

Potential mitigations for the identified risks and threats under the proposed Digitalised Business Model for PP Pampered Pets.

1. Implementation of the cyber security governance framework to guide in addressing digitalisation risks.
2. Adopting public/private/ hybrid cloud technologies (Deloitte, 2018).
3. Implementation of a secure digital payment gateway following PCI-DSS guidelines.
4. Enabling implementation and adoption of Artificial Intelligence/automation (e.g. SIEM or SOAR products from managed security providers)
5. Implement user authentication technologies and access control mechanisms to prevent unauthorised access (mitigating Spoofing and Elevation of Privilege).
6. Implementation of firewall and intrusion detection system to monitor and block malicious traffic, mitigating Denial of Service attacks.
7. Regularly backup data and test the recovery process to ensure business continuity and disaster recovery.

Despite challenges and risks, Pampered Pets should embrace digitalisation for growth beyond its local catchment area, ensuring resilience even during natural disasters or crises like COVID-19. This move will boost operational efficiency, cross-border sales, customer engagement, and competitiveness.

Conclusion

Pet product e-commerce research by Jacobovitz et al. (2022) indicates that the online presence of similar pet businesses like PP can boost annual business growth by at least 10%, reaching 50% within 5 years with efficacious implementation. Shifting to an international supply chain may not yield tangible cost reduction due to higher taxes on the importation of raw materials. We therefore conclude that digitalisation will enhance sales and profit margins. We recommend adopting a hybrid business model to prevent potential 33% customer losses.

References

1. BigCommerce (N.D.). PCI Compliance: A Guide to Meeting Today's Requirements. Available from: https://www.bigcommerce.co.uk/articles/ecommerce/pci-compliance/. [Accessed September 14 2023].
2. Deloitte (2018) Managing Risk in Digital Transformation. Available from: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_managing_risk_in_digital_transformation_112018.pdf [Accessed September 16 2023].
3. Digital Adoption (2023). Data Lifecycle Management: Everything You Need To Know. Available from: https://www.digital-adoption.com/data-lifecycle-management/. [Accessed September 14 2023].
4. ICT Instituite (2021). Example Risk Register. Available from: https://ictinstitute.nl/wp-content/uploads/2021/01/Example-risk-register.png. [Accessed September 14 2023].
5. Jacobovitz, S. & Jolly, N. (2022). The impact of e-commerce on the pet sales landscape. Available from: https://www.dv
6. m360.com/view/the-impact-of-e-commerce-on-the-pet-sales-landscape. [Accessed September 17 2023].
7. Juma.A,(2022). Ineed. Qualitative Risk Analysis: Definition, Methods, and Steps. Available from: https://www.indeed.com/career-advice/career-development/qualitative-risk-analysis [Accessed September 15, 2023].
8. Microsoft (2023). ISO/IEC 27001:2013 Information Security Management Standards Available from: https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-27001. [Accessed September 13 2023].

9. NIST SP 800-97 (2007). Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Available from: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-97.pdf. [Accessed September 12 2023].
10. Oracle (N.D.). What Is a Warehouse Management System (WMS)?. Available from: https://www.oracle.com/uk/scm/logistics/warehouse-management/what-is-warehouse-management/. [Accessed September 16 2023].
11. Orbussoftware (N.D.). The 5 Key Business Impact Analysis Steps. Available from: https://www.orbussoftware.com/resources/blog/detail/the-5-key-business-impact-analysis-steps#:~:text=The%20majority%20of%20businesses%20will,%2C%20Production%20output%2C%20and%20Environmental. [Accessed September 14 2023].
12. Petersen, R. et al. (NIST: 2020). Workforce Framework for Cybersecurity (NICE Framework). Available from: https://csrc.nist.gov/pubs/sp/800/181/r1/final. [Accessed September 12 2023].
13. SANS (2022). SANS 2022 Security Awareness Report: Human Risk Remains the Biggest Threat to Your Organization’s Cybersecurity. Availalbe from: https://www.sans.org/press/announcements/sans-2022-security-awareness-report-human-risk-remains-biggest-threat-organizations-cybersecurity/. [Accessed September 16 2023].
14. Shotstack. A,(2014). Threat Modeling : Designing for Security.Available from: https://ebookcentral.proquest.com/lib/universityofessex-ebooks/reader.action?docID=1629177[Accessed September 9 2023].

15. Spears, J. & Barki, H. (2010). User Participation in Information Systems Security Risk Management. MIS Quarterly 34(3): 503. Available from: https://www-jstor-org.uniessexlib.idm.oclc.org/stable/25750689 [Accessed August 21 2023]
16. Sphera (N.D.). Digital Transformation Across the Complete Asset Lifecycle. Available from: https://sphera.com/digital-transformation-across-the-complete-asset-lifecycle/. [Accessed September 14 2023].
17. University of Essex Online Lecture-cast 3 (2023). Threat Management and Modelling. Available from: https://www.my-course.co.uk/Computing/Cyber%20Security/SRM/SRM%20Lecturecast%202/content/index.html#/lessons/ieO_uo7-67lmlblEhYZpQttFUJjRJ6C8[Accessed August 29 2023].